Joint Pub 3-10.1

Joint Tactics, Techniques, and Procedures for Base Defense

23 July 1996

PREFACE

1. Scope

This publication sets forth the joint tactics, techniques, and procedures (JTTP) necessary for the defense of joint and single-Service bases outside the continental United States (CONUS) and outside the states of Alaska and Hawaii. It expands upon the doctrine set forth in Joint Pub 3-10, "Doctrine for Joint Rear Area Operations." The focus is on establishing and maintaining security of joint and single-Service bases in a joint rear area and providing guidelines for base commanders for coordinating and integrating security and defense of their bases with their other responsibilities. This publication should be supplemented with Service manuals that provide more detail on the measures necessary to secure and defend bases. This publication:

a. Prescribes the command and control arrangements between bases, base clusters, and their higher headquarters.

b. Describes the responsibilities of base and base cluster commanders and commanders of units and activities within such bases.

c. Sets forth procedures for base defense and security from the standpoints of operational concepts, analysis, planning, command and control, intelligence, communications, and host-nation support (HNS).

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth doctrine and selected tactics, techniques, and procedures to govern the joint activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for US military involvement in multinational and interagency operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders and prescribes doctrine and selected tactics, techniques, and procedures for joint operations and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the joint force commander (JFC) from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall mission.

3. Application

a. Doctrine and selected tactics, techniques, and procedures and guidance established in this publication apply to the commanders of combatant commands, subunified commands, joint task forces, and subordinate components of these commands. These principles and guidance also may apply when significant forces of one Service are attached to forces of another Service or when significant forces of one Service support forces of another Service.

b. The guidance in this publication is authoritative; as such, this doctrine (or JTTP) will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence for the activities of joint forces unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders

of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable.

For the Chairman of the Joint Chiefs of Staff:

CARLTON W. FULFORD, JR.
Major General, USMC
Vice Director, Joint Staff

TABLE OF CONTENTS

PAGE

EXECUTIVE SUMMARY vii

CHAPTER I
JOINT REAR AREA CONCEPTS

- General I-1
- Background I-1
- Levels of Response I-5
- Legal Constraints I-6
- Public Affairs I-7

CHAPTER II
COMMAND AND CONTROL

- General II-1
- Responsibilities II-1
- Operations Centers II-8
- Assigned Areas of Responsibility II-10
- Liaison II-10
- Nonmilitary Agencies II-10

CHAPTER III
COMMUNICATIONS

- General III-1
- Planning and Construction Considerations III-1
- Capabilities III-2
- Base Defense Communications System III-2
- Base Defense Communications Nets III-3

CHAPTER IV
BASE DEFENSE OPERATIONS

- General IV-1
- The Fundamentals of Base Defense IV-1
- Defensive Factors IV-3
- Base Commander's Intelligence Responsibilities IV-6
- Planning IV-7
- Evacuation IV-16

CHAPTER V
HOST-NATION SUPPORT

- General V-1
- Planning for HNS of Base Defense V-1
- Base Defense Coordination V-1
- Facilities and Systems V-2
- Supplies, Services, and Equipment V-2
- Command and Control V-3
- NBC Defense V-3
- Training V-3
- Intelligence V-3
- Civil Affairs V-3
- Psychological Operations V-4

APPENDIX

A Maritime-Land Interface A-1
B Nuclear, Biological, Chemical Defense B-1
C Air and Missile Defense C-1
D Base Defense Operations Center D-1
E Sample Base Defense Plan E-1
F Security F-1
G Terrorism G-1
H Specialized Equipment and Materiel H-1
J References J-1
K Administrative Instructions K-1

GLOSSARY

Part I Abbreviations and Acronyms GL-1
Part II Terms and Definitions GL-3

FIGURE

I-1 Joint Rear Area Operations I-2
I-2 Threats to the Joint Rear Area I-5
II-1 Joint Rear Area Command and Control Network for Security Operations with Army Component Commander Designated as Joint Rear Area Coordinator II-3
II-2 Joint Rear Area Command and Control Network for Security Operations with Joint Rear Area Coordinator Selected from the Joint Force Commander's Headquarters II-4
II-3 Notional Geographical Organization—JRA II-5
II-4 Tenant Unit Commander's Responsibilities II-7
II-5 Intelligence and Counterintelligence Sources of Information II-10
III-1 Base Defense Communications System Characteristics III-2
III-2 Notional Base Defense Communications Links III-4

IV-1 Fundamentals of Base Defense IV-1
IV-2 Defensive Factors IV-3
IV-3 Response Force Tactical Control to Base Commander (Response Force Committed While Base Defense Forces are Engaged with a Threat) IV-9
IV-4 Selected Base Defense Force TACON to Response Force Commander (Response Force Committed Prior to Base Defense Forces Engaging the Threat) IV-10
IV-5 Base Defense Force Operational Control to the Tactical Combat Force Commander During Level III Operations IV-11
IV-6 Work Priorities in Base Defense IV-13
IV-7 Physical Perimeter Defense Measures IV-15
V-1 Planning for Host-Nation Support in Base Defense V-2

Intentionally Blank

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Discusses Joint Rear Area Concepts**
- **Covers General Responsibilities for Command and Control of Joint Rear Area Concepts**
- **Addresses the Planning and Construction Considerations for Communication**
- **Provides the Fundamentals of Base Defense Operations**
- **Discusses Host-Nation Support**

General Considerations for Joint Rear Area Concepts

A joint rear area (JRA) is a specific land area within a joint force commander's operational area designated to facilitate protection and operation of installations and forces supporting the joint force.

The joint rear area (JRA) is organized into areas of operation (AOs), which may in turn be subdivided into smaller AOs to facilitate control of the defense. Each base has a corresponding AO which includes the base itself. **To facilitate the span of control for area commanders, bases may be grouped into base clusters.** Each base cluster's AO encompasses those bases included in the cluster. In the early stages of theater development, rear area bases can be highly vulnerable. The availability and effectiveness of host nation (HN) contributions to base defense must be assessed. The joint force commander (JFC) may be required to adjust the concept of operations, sequencing, and unit missions.

The effective implementation of JRA doctrine and the joint tactics, techniques and procedures for base defense protects the JRA and the joint force.

The broad functions of activities assigned to bases in the JRA include but are not limited to: force protection; security; command, control, communications, and computers; intelligence; sustainment; movements; medical support; infrastructure development and area management; and host-nation support with host-nation territorial organizations and third country allies. **Threats to bases in the rear area are categorized by the levels of defense required to counter them.** Each level, or all levels simultaneously, may exist in the JRA. Emphasis on specific base defense and security measures may depend on the anticipated threat level. **The commander's intent must not be in conflict with legal constraints.** Commanders at all levels must be well-informed on the legal aspects of the use of force. The laws and rules that

regulate the status and activities of the forces across the range of military operations include international agreements, US laws, host-nation laws, the law of war and rules of engagement. Public affairs and civil affairs personnel must work together to gain public support and understanding of the activities, especially from those on or near the base, to ensure that all security requirements and precautions are implemented.

Command and Control of Joint Rear Area Operations

Unity of effort is as essential for the forces in the JRA as it is for the combat forces. Clear-cut procedures for authority and responsibility must be established for the successful execution of missions by the units and activities in the JRA and for the security and survival of the bases housing those units and activities.

The geographic combatant commander is ultimately responsible for all JRA operations conducted in the theater, including maintaining the security of the command and protecting US possessions and bases against attack or hostile incursions; assigning responsibility for defense; ensuring that appropriate command relationships are established; and determining the classification of bases in the theater (single-Service or joint base). Subordinate JFCs may organize by Service component or function. Supporting combatant commanders provide support to the theater and may establish facilities or occupy bases within the theater. The JFC must ensure that these facilities or bases are adequately defended. Command and coordination relationships between those elements and the area or base commanders subordinate to the JFC will be defined by orders or memorandums of agreement.

A joint rear area coordinator may be created to coordinate the overall securing and intelligence support of the JRA in accordance with JFC directives and priorities. **Component commanders** may be given responsibility for overall defense of designated areas and bases within the JRA. **Area commanders** are responsible for AOs, including land areas which they assign to Army or Marine Corps components. **Base cluster commanders** are responsible for coordinating the defense of bases within the base cluster and integrating base defense plans into both a base cluster defense plan and the area defense plan. **Tenant unit commanders** participate in the preparation of base defense plans; provide, staff, and operate base defense facilities; conduct individual and unit training; and provide secure and other communications systems within the base. **Response force commanders** are in charge of a mobile force designated (usually by the area commander) to deal with Level II threats. Response force commanders may be put under the tactical control of commanders of threatened bases. **Tactical combat force (TCF) commanders** are responsible for a combat unit, with appropriate combat support and combat service support assets, which is assigned the mission of defeating Level III threats. The threat requiring

the commitment of a TCF is usually of such magnitude that several bases or base clusters are threatened. The TCF commander may be directly subordinate to the JFC or to a component commander.

Various operations centers must be coordinated for joint rear area operations.

Joint rear tactical operations centers, rear area operations centers, rear tactical operations centers, base cluster operations centers, and base defense operations centers (BDOC) need to be set up to support the mission and to ensure security of the joint rear area.

Communications for Joint Base Defense

Effective communications for joint base defense present numerous challenges. All component communications systems on the base, both secure and unsecure, must be compatible to facilitate effective command and control of defense and security operations.

Base communications facilities for both defense and primary missions must be planned, coordinated, and established. Existing base communications facilities are used to the maximum extent possible for base defense; however, a separate communications system may be necessary. Wire is the normal means of internal base communications between fixed sites like sentry posts, checkpoints, and the BDOC. When dealing with Level II and Level III threats, radio will become the primary carrier for tactical traffic. Plans should be developed to provide for alternate means of communications, such as using community communications systems, base cable, armed forces, or civilian-owned radio broadcast stations and television. **A secure, robust, redundant, reliable communications system is required** between defense units, staff elements, headquarters, and operations centers.

Base Defense Operations

The base commander organizes and controls all forces assigned to the base to capitalize on their capabilities. These forces must be trained, organized, and equipped to contribute to the defense of the base.

The general characteristics of defensive operations are: to understand the enemy; see the battlefield; use the defenders' advantages; concentrate at critical times and places; conduct counterreconnaissance and counterattacks; coordinate critical defense assets; balance base security with political and legal constraints; and know the law of war and rules of engagement. The primary mission of the base is to support joint force objectives. Essential actions of the defense force are to detect, warn, deny, destroy, and delay. Every intelligence and counterintelligence resource available to the base commander should be used to determine enemy capabilities and intentions. **The base commander must make the best use of the terrain within the commander's AO.** Commanders analyzing terrain must consider all its military aspects from the standpoints of both defenders and the enemy, including observation and fields of fire, cover and concealment, obstacles, key terrain, and avenues of approach. Additionally, commanders must analyze

the effects of weather on both defender and enemy weapons systems and tactics. Weather and visibility conditions can have significant effects on ground, air, and maritime operations. The base commander is responsible for ensuring that intelligence functions are performed in a timely manner.

Upon notification by a base cluster commander that a threat exceeds a base's defense capabilities, the area commander commits the response forces or requests the commitment of a tactical combat force.

The response forces may include mobile reserves, antiarmor weapons, indirect fire support, and other aviation support. Obstacles and mines, communications countermeasures, security measures, counter attack plans, area damage control measures, air and missile defense measures, nuclear, biological, and/or chemical defense measures, threat response contingency plan, and physical facilities must all be considered. **In extreme situations, it may be necessary to evacuate a base or part of a base** or to move essential base activities elsewhere in the JRA to perform their functions with less enemy interference. Plans should include the identification of bases most at risk, the advantages and disadvantages of evacuation, and the conduct of evacuation operations.

Host-Nation Support During Joint Rear Area Operations

Host-nation support is based on bilateral diplomatic agreements that commit the host nation to provide specific support under prescribed conditions.

Host-nation support (HNS) enhances the abilities to US forces to perform their missions. HNS can reduce requirements for US personnel, materiel, and services, allowing more flexibility in assigning forces. HNS is essential when political agreements limit the numbers of US personnel on bases. When the forces of the United States, HN, and third country allies and coalition partners occupy bases together, special consideration must be given to the synchronization of command and control (C2) and the defense capabilities from every available source. HN government agencies build, operate, and maintain facilities and systems (utilities, telephone networks, police, fire fighters, facilities for hospitals, headquarters and other maintenance shops). Supplies, service and equipment are acquired from US, HN, or third country contractors. C2 is retained by the US and HN commanders for their respective units.

CONCLUSION

This publication sets forth the joint tactics, techniques, and procedures necessary for the defense of joint and single-Service bases outside the continental United States and outside the states of Alaska and Hawaii. This publication prescribes the command and control arrangements between bases, base clusters, and their higher headquarters; describes the responsibilities of base and base cluster commanders and

commanders of units and activities within such bases; and sets forth procedures for base defense and security from the standpoints of operational concepts, analysis, planning, C2, intelligence, communications, and HNS.

Intentionally Blank

CHAPTER I
JOINT REAR AREA CONCEPTS

"What boots it at one gate to make defense,
And at another to let in the foe?"

John Milton
Samson Agonistes, 1671

1. General

a. This chapter describes the joint rear area (JRA) in terms of its geography and functions. It discusses the levels of threat as they affect rear area operations and base defense and recognizes that effective defense may require careful integration of air and surface forces, because the threat will probably consist of integrated air and surface operations. **The JRA concept is applicable across the range of military operations.** This chapter also sets forth the legal aspects that commanders must consider.

b. The rear area of a joint force may be vulnerable to attacks by modern enemy forces with sophisticated surveillance devices, accurate weapon systems, and transport assets capable of inserting forces behind friendly combat formations. Rear area installations also may be the targets for indigenous elements capable of the full spectrum of unconventional operations ranging from crime, sabotage, and terrorism to large-scale raids. **The JRA contains units and facilities from all components that are critical to the theater or joint operations area.** These units and facilities are organized into bases to enhance their effectiveness and security.

2. Background

a. **Introduction. A JRA is a specific land area within a joint force commander's (JFC's) operational area designated to facilitate protection and operation of installations and forces supporting the joint force.**

b. **Location and Configuration of the JRA**

- This publication concentrates on bases in the JRA. The tactics, techniques, and procedures set forth also can apply to bases established in the combat zone.

- **The JRA does not normally include a naval area of operations (AO).** When a naval AO and a JRA meet along a coastline, the high water mark will normally designate the boundary between the two. Ports and harbors, though not the built-up areas around them, are normally included in the naval AO. Ports and harbors on the coastline of a JRA may interface with bases necessary for the simultaneous support of land, air, and maritime operations. See Appendix A, "Maritime-Land Interface."

- **The JRA is organized into assigned AOs**, which may in turn be subdivided into smaller AOs to facilitate control of the defense. **Each base is assigned an AO** which includes the base itself. To facilitate the span of control for area commanders, **bases may be grouped into base clusters**. Each base cluster's AO encompasses those bases included in the cluster.

c. **Evolution of the JRA**

- In the early stages of theater development, rear area bases can be highly vulnerable. **From the outset, base AOs must be clearly defined and**

rear area security forces must be available. The availability and effectiveness of host nation (HN) contributions to base defense must be assessed. Based on this assessment, the JFC may be required to adjust the concept of operations, sequencing, and unit missions.

- The development of base defense procedures during theater development should be directed toward the establishment of a stable JRA supporting the JFC's concept of operations.

d. **JRA Operations.** The implementation of JRA doctrine and joint tactics, techniques, and procedures for base defense protects the JRA or supports the joint force. **The broad functions of activities assigned to bases in the JRA are shown in Figure I-1 and include** but are not limited to the following.

- **Force Projection.** Particularly where air assets are involved, the most important missions of some rear area bases may be to project combat power in support of the JFC's objective.

- **Security.** Designated rear area units contribute to the security of the entire joint force. For example, bases may contain aircraft or missiles capable of performing defensive counterair missions, radars, and other equipment critical to air defense or units conducting counterintelligence (CI), executing electronic protection, or guarding enemy prisoners of war (EPWs).

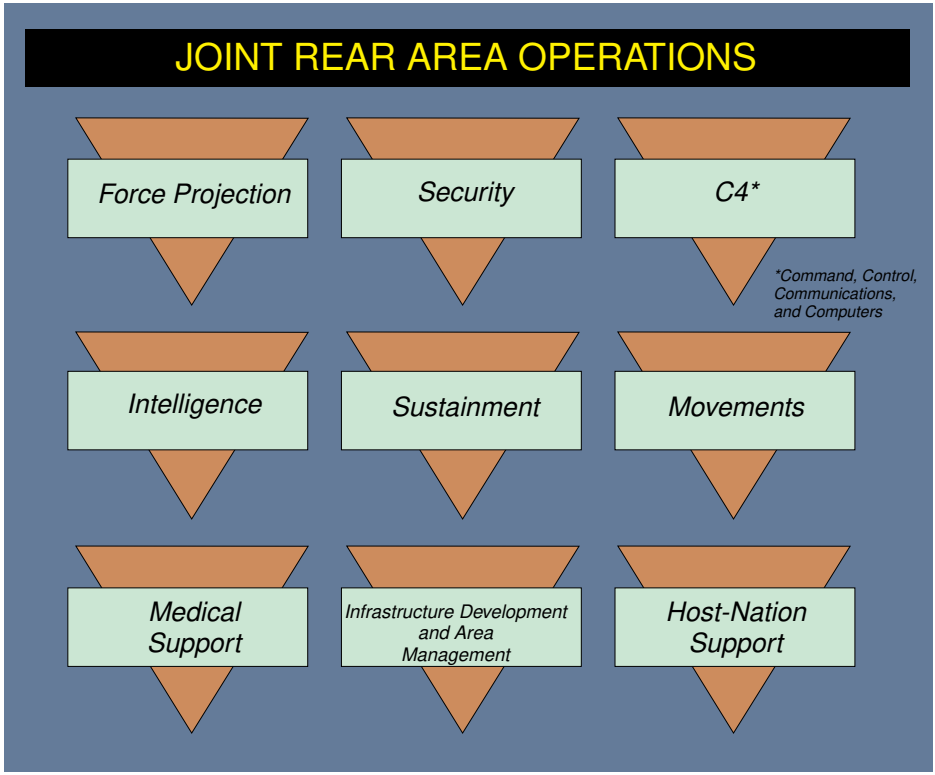


Figure I-1. Joint Rear Area Operations

- **Command, Control, Communications, and Computers (C4).** Bases containing headquarters and signal centers at all levels may be among the largest and most critical installations in the JRA.

- **Intelligence.** Bases in the JRA may contain intelligence centers and electronic facilities designed to interface with forward-based, airborne, or space-based sensors.

- **Sustainment.** The fighting forces depend upon the combat service support forces, materiel, and resources to sustain operations on the bases throughout the JRA.

- **Movements.** Joint movement centers, rail terminals, and seaports and aerial ports of debarkation occupy bases in the JRA. Lines of communications between bases and from the JRA to combat forces also must be secured.

- **Medical Support.** Medical facilities in the JRA are special sustainment bases that should be situated away from all legitimate military targets to avoid endangerment. The Geneva Conventions prescribe the security and defensive measures, as well as the protections, applicable to medical facilities and their personnel.

- **Infrastructure Development and Area Management.** Construction sites and facilities of construction units involved in base development must be considered as bases for defense purposes. All units and facilities in the JRA must be properly positioned and adequately protected to maximize their effectiveness. During large joint operations, whether at a seaport or a land-based location, the Army Material Command may have extensive ongoing contractor support operations. Allowance must be made for their presence and for the resulting required special protective measures.

- **Host-Nation Support (HNS).** The HN, in accordance with negotiated agreements, will assist in performing defense functions within the JRA. US forces may also, in coordination with the HN, be responsible for the defense of HN facilities on US bases. Civilian agencies of the US Government, such as the Drug Enforcement Administration and Agency

Rear area security forces must be available to provide protection at aerial ports of debarkation.

for International Development located in the HN, may also occupy US or HN bases in the JRA.

e. **Multinational Considerations**

- **Host-Nation Territorial Organization.** The JRA normally will be in sovereign territory presided over by viable and capable HN governments. These governments, represented by their forces and law enforcement agencies, generally will have responsibility for many rear area functions. The JFC will coordinate US HNS requirements with HN commands.

- **Allies and Coalition Partners.** When the forces of another allied or coalition nation share base facilities with the United States and the HN, **unity of effort must be achieved by cooperative measures**. The presence of allied and coalition forces and facilities in the JRA will have its impact on virtually every aspect of base defense, including command and control arrangements, communications, fire support planning and integration, location of various national units, rules of engagement (ROE), establishment of a tactical combat force (TCF), liaison, and the establishment of the bases and base clusters themselves. Multinational considerations are discussed in Joint Pub 3-10, "Doctrine for Joint Rear Area Operations."

BASE DEFENSE BEGINS - WWI

On the 24th of August 1914 Captain H.C. Jackson and Lt. E. L. Conran of the Royal Flying Corps were on an observation patrol near Tournai, in Flanders. About noon, they spotted three parked German aircraft on an airfield outside the town of Lessines. Lieutenant Conran banked the plane for a closer look, and as they passed one of them threw a bomb overboard. The attack caused no damage and was notable only because it was one of the first air attacks on an enemy air base. Neither bombardment nor attack was the mission of flyers early in World War I. They were observers, sent to report on troop movements, supply and artillery positions, and the like. The most important function of aircraft units during the early years of fighting was to spot for and adjust gun fire. If these early aviators used bombs, they were often nothing more than hand grenades or containers of gasoline thrown from the cockpit. The pilot or observer usually released the first externally mounted bombs by cutting the retaining strings, and their destructive power was quite limited. Not to be outdone by the British, the Germans attacked an airfield near Compiegne on August 29th. Again, there was no damage.

As the war continued into the autumn, it grew in scope. Germany introduced zeppelins to the conflict and with their use gained the ability for both long range reconnaissance and bombardment. In September 1914, the British Admiralty concluded that German zeppelins posed a threat to the British fleet as well as to targets in England. The Royal Navy Air Service's (RNAS) squadron at Dunkirk received orders to attack the zeppelin bases. All the airships within 100 miles were to be destroyed. On September 22, 1914, the RNAS launched the first raid on the zeppelin hangers at Dusseldorf; it failed when the bombs fell short of the target or did not explode. On October 8, two attacks by a single aircraft at Cologne were more successful. They destroyed a zeppelin, a zeppelin shed, and a machine shop. The pilots met heavy ground fire from

rifles and antiaircraft guns. One airplane was badly damaged, but both pilots returned safely. The destruction at Cologne pleased one man ever on the lookout for new ideas: Winston Churchill, then first Lord of the Admiralty, encouraged more attacks and was, in fact, an early believer in destroying an enemy's air forces on the ground at his bases.

SOURCE: John F. Kries, Air Warfare and Air Base Defense Office of Air Force History, 1988

3. Levels of Response

Threats to bases in the rear area are categorized by the levels of defense required to counter them. Each level, or all levels simultaneously, may exist in the JRA. Emphasis on specific base defense and security measures may depend on the anticipated threat level. Responsibilities for dealing with threats at each level are discussed in Chapter II, "Command and Control." (See Figure I-2.) The threat levels that follow also are discussed in detail in Joint Pub 3-10, "Doctrine for Joint Rear Area Operations."

a. **Level I threats** can be defeated by base or base cluster self-defense measures.

b. **Level II threats** are beyond base or base cluster self-defense capabilities but can be defeated by response forces, normally military police (MP) units assigned to area commands with supporting fires.

c. **Level III threats** necessitate the command decision to commit a TCF. Level III threats, in addition to major ground attacks, include major attacks by aircraft and theater missiles armed with conventional weapons or

THREATS TO THE JOINT REAR AREA

THREAT LEVEL	EXAMPLES	RESPONSE
LEVEL I	Agents, saboteurs, sympathizers, terrorists	Unit, base, and base cluster self-defense measures
LEVEL II	Small tactical units, unconventional warfare forces, guerrillas	Self-defense measures and response force(s) with supporting fires
LEVEL III	Large tactical force operations, including airborne, heliborne, amphibious, infiltration, and major air operations	May require timely commitment of tactical

Figure I-2. Threats to the Joint Rear Area

nuclear, biological, and chemical (NBC) weapons. Appendix B, "Nuclear, Biological, and Chemical Defense," and Appendix C, "Air and Missile Defense," contain special considerations for the defense of bases against NBC and air threats.

4. Legal Constraints

A commander's intent must not be in conflict with legal constraints. **Commanders at all levels must be well-informed on the legal aspects of the use of force.** The types of guidance relevant to the use of force include international law, US law, HN law, law of war, ROE, and United Nations (UN) sanctions (as applicable). Together, these laws and rules regulate the status and activities of the forces across the range of military operations.

a. **International Agreements.** International agreements are **the most important source of international law** applicable to US, multinational, and HN forces. They prescribe most of the reciprocal rights, powers, duties, privileges, and immunities of the US forces stationed abroad and of the governments of the host and allied nations and their respective armed forces. They also may regulate, to some extent, the relationship between the opposing parties in internal conflicts. The Armed Forces of the United States are committed to conducting defense operations according to the applicable provisions of the law of war, including those of the Hague and Geneva Conventions. **The four relevant categories are those concerning:**

- **Law of war;**
- **Security assistance agreements;**
- **Status-of-forces agreements (SOFA); and**
- **HNS agreements.**

b. **US Laws. US forces overseas follow US law** as expressed in statutes, Executive Orders, Department of Defense (DOD) directives and instructions, and military regulations. Directives issued by the geographic combatant commander and by the component commanders are subject to applicable SOFAs or similar agreements. Publications containing applicable US laws and SOFAs should be on file at the security assistance office or with the command legal adviser. Some SOFAs and similar agreements are classified.

c. **Host-Nation Laws. Sovereign HN laws apply to all US forces stationed in that country to the extent provided for by international agreements.** Neither US nor HN laws have priority over the law of war; for example, commanders are responsible for the humane care of EPWs regardless of HN policies. Such laws emanate from the various levels of government and from the agencies functioning at each echelon. US advisers, commanders, staff officers, and Service members must understand critical HN laws and the provisions of DOD and Service policies concerning HNS.

d. **Law of War.** The law of war (also called the law of armed conflict) and the obligations of the US Government under that law govern the conduct of US forces. **US commanders will ensure that the DOD Law of War Program is implemented** in accordance with directives and procedures.

- **Treatment of Combatants.** During a war, the treatment of combatants is governed by the law of war, the 1949 Geneva Conventions, and relevant HN and US domestic laws.
- **Treatment of Insurgents.** For insurgents held in US military custody, US policy requires and directs humane care and treatment from the moment they are detained until they are released or repatriated. This policy also applies to all detained or interned personnel. In

combating an insurgency, defenders must accord humane treatment to any civilians involved and scrupulously observe the law to demonstrate US Government concern for individuals.

- **Treatment of Prisoners.** The treatment of EPWs is governed by the 1949 Geneva Conventions. Whether captives are entitled to EPW status will be determined in accordance with the rules and procedures of the Geneva Conventions.

- **Protection of Noncombatants.** These responsibilities under the law of war are especially applicable in or near bases in the rear area. In addition to taking measures to avoid civilian casualties during combat operations, commanders have a special responsibility to safeguard the US and HN civilians employed in support of base missions. Civilian protection from enemy threats must take a high priority in base defense and security plans.

e. **Rules of Engagement.** ROE are directives issued by competent military authority that delineate the circumstances under which US forces will initiate or continue combat engagement with other forces. **Geographic combatant commanders establish ROE based upon guidance provided by the National Command Authorities through the Chairman of the Joint Chiefs of Staff (CJCS).** CJCS Instruction 3121.01, "Standing Rules of Engagement for US Forces," should also be consulted.

5. Public Affairs

The public affairs (PA) **objective for the base is to gain public support and understanding, especially from those on or near the base**. The base commander should encourage a strong and active command information program to ensure the fullest dissemination of security requirements, safety precautions, and other essential matters. Flexible public information and community relations programs should be established to provide maximum disclosure of information within the constraints imposed by safety and security requirements. **Close coordination with civil affairs (CA) and psychological operations (PSYOP) personnel is also encouraged** to better meet external information requirements. PA activities must be coordinated with other staff agencies to ensure that all actions are complementary.

Intentionally Blank

CHAPTER II
COMMAND AND CONTROL

"Our army would be invincible if it could be properly organized and officered."

Robert E. Lee
To "Stonewall" Jackson, 1862

1. General

Unity of effort is as essential for the forces in the JRA as it is for the combat forces. Clear-cut procedures for authority and responsibility must be established for the successful execution of missions by the units and activities in the JRA and for the security and survival of the bases housing those units and activities. These activities may involve interaction with host-nation noncombatants, United Nations personnel, nongovernmental organizations, and private voluntary organizations. Refer to Joint Pub 3-08, "Interagency Coordination During Joint Operations," for more information on interactions with these agencies. This chapter sets forth the responsibilities, facilities, geographic organization, and liaison requirements necessary to command, coordinate, and synchronize the defense of bases within the JRA.

2. Responsibilities

a. **Geographic Combatant Commander.** A geographic combatant commander (CINC), as commander of a unified command, **is ultimately responsible for all JRA operations conducted in the theater**. These responsibilities include the following.

- **Maintaining the security of the command and protecting US possessions and bases** against attack or hostile incursions.

- **Assigning responsibility for defense of the JRA and either establishing the method of command or coordination** to be exercised or delegating that authority to a subordinate JFC.

- **Either ensuring that appropriate command relationships between subordinate area and local base defense commanders are established** and that local defense areas are delineated, or delegating that authority to a subordinate JFC.

- **Determining the classification of bases in the theater**, unless determined by higher authority. A base may be either:

  •• A single-Service base; or

  •• A joint base. A joint base may be either: (1) One in which one Service component has primary interest; or (2) One in which two or more Service components have coequal interest.

b. **Joint Force Commander.** The term "joint force commander" is used to refer to the commander of a combatant command, subordinate unified command, or joint task force. JFCs have the authority to organize forces to best accomplish the assigned mission based on their concept of operations. See Joint Pub 0-2, "Unified Action Armed Forces (UNAAF)" for further amplification.

c. **Supporting Combatant Commanders. Elements** of combatant commands **providing support** to the theater, such as US Transportation Command and US Space Command, **may establish facilities or occupy bases within the theater**. **The JFC must ensure that these facilities or bases**

are adequately defended. Command and coordination relationships between those elements and the area or base commanders subordinate to the JFC will be defined by orders or memorandums of agreement. Coordination must include sharing of intelligence information, because supporting CINC operations are often planned outside the theater.

d. **Joint Rear Area Coordinator. The JFC normally designates a component commander or a member of the joint force headquarters staff as the joint rear area coordinator (JRAC).** The JFC considers mission requirements, force capabilities, the nature of the JRA, and the threat in making the selection. **The JRAC is responsible for coordinating the overall security of the JRA in accordance with JFC directives and priorities.** The JRAC coordinates with appropriate JRA commanders to ensure that they maintain the security of their AOs to facilitate sustainment, HNS, infrastructure development, and movements of the joint force. The JRAC also ensures that commanders establish reliable intelligence support and practice area management within their AOs with due consideration of security requirements. The JRAC establishes secure and survivable communications with all forces and commands operating in or transiting the JRA. The JRAC is also responsible for ensuring that the surface area security requirements and priorities for the JRA are integrated in the overall security requirements of the joint force and are coordinated with the area air defense commander (AADC). However **in cases of Level III threat or other emergencies, the JFC may assign a subordinate commander the responsibility to counter the threat and restore JRA security**. In this case, the assigned subordinate commander would assume the JRAC's responsibilities and be tasked to restore JRA security. The JRAC will support any requirements requested by the assigned subordinate commander. This option would be exercised for the duration of the threat or as directed by the JFC. **The AADC is responsible for the security of the airspace above the JRA.** Joint Pub 3-10, "Doctrine for Joint Rear Area Operations," includes a detailed discussion of JRAC responsibilities. Figures II-1 and II-2 depict notional JRA command and control (C2) networks, with options for the selection of the JRAC.

e. **Component Commanders.** The JFC may exercise command through Service component or functional component commanders. Although this publication is based on a Service component framework, the principles can be applied within a functional structure. **Component commanders may be given responsibility for overall defense of designated areas and bases within the JRA.** Joint Pub 3-10, "Doctrine for Joint Rear Area Operations," describes component relationships in the JRA.

f. **Area Commanders.** Service component commanders with area responsibilities subdivide their areas into AOs for which subordinate commanders are responsible. **Land areas in the JRA are normally assigned to Army or Marine Corps components.** Although the responsibilities of area commanders do not vary, differences between Army and Marine Corps organizations may dictate some differences in the JRA organization. Figure II-3 shows a notional geographic organization for a JRA.

- **Army forces in the JRA can constitute a theater army whose commander, if designated the JRAC, is responsible for the surface security of the entire JRA.** The Commander, Army Forces, organizes by assigning to one or more theater army area commands (TAACOMs) the defense and security responsibilities for appropriate subdivisions of the JRA. TAACOM AOs will be further subdivided and assigned to area support groups (ASGs). ASG

Figure II-1. Joint Rear Area Command and Control Network for Security Operations with Army Component Commander Designated as Joint Rear Area Coordinator

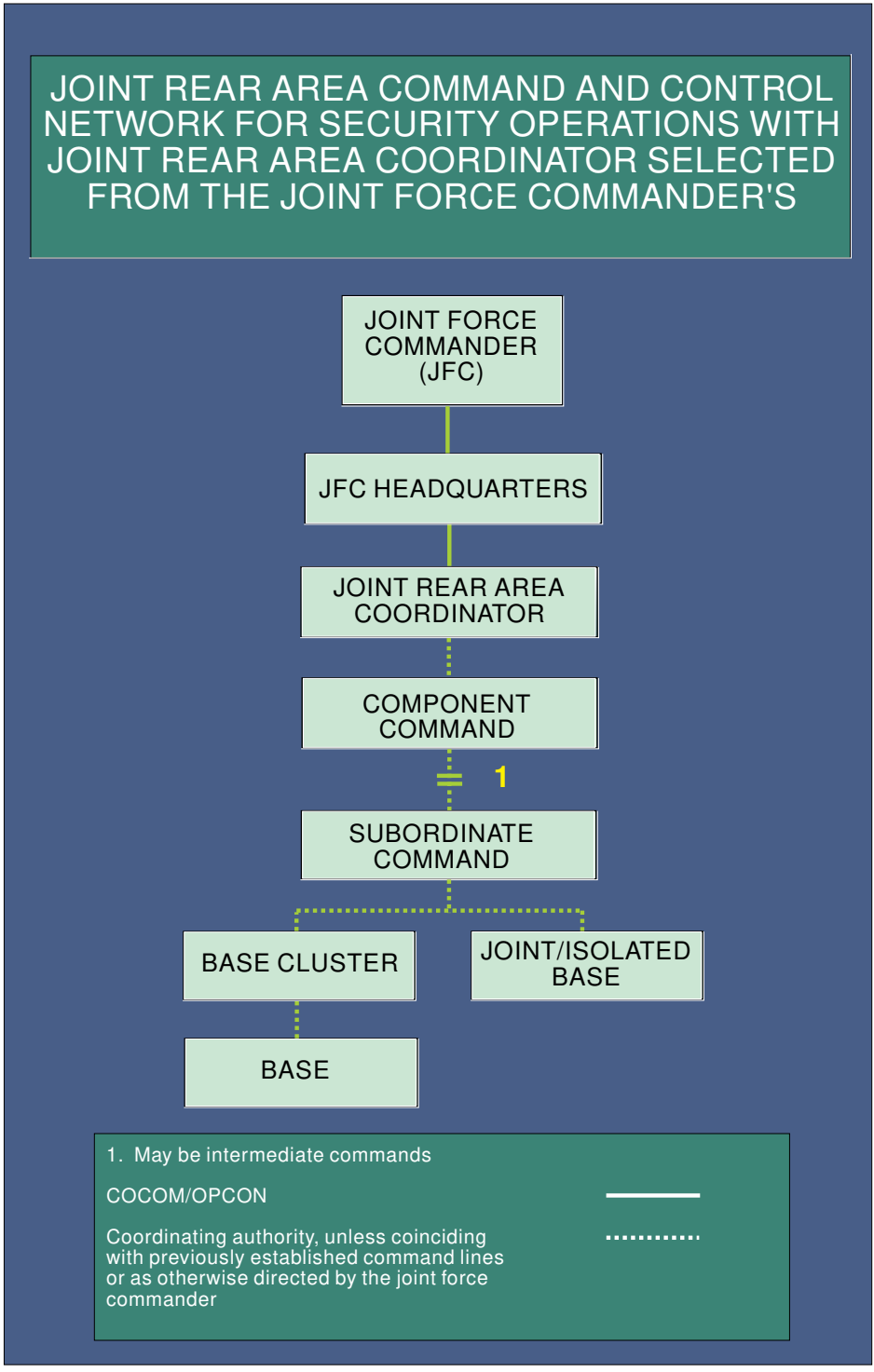

JOINT REAR AREA COMMAND AND CONTROL NETWORK FOR SECURITY OPERATIONS WITH JOINT REAR AREA COORDINATOR SELECTED FROM THE JOINT FORCE COMMANDER'S
JOINT FORCE COMMANDER (JFC)
JFC HEADQUARTERS
JOINT REAR AREA COORDINATOR
COMPONENT COMMAND
1
SUBORDINATE COMMAND
BASE CLUSTER
JOINT/ISOLATED BASE
BASE
1. May be intermediate commands
COCOM/OPCON
Coordinating authority, unless coinciding with previously established command lines or as otherwise directed by the joint force commander

Figure II-2. Joint Rear Area Command and Control Network for Security Operations with Joint Rear Area Coordinator Selected from the Joint Force Commander's Headquarters

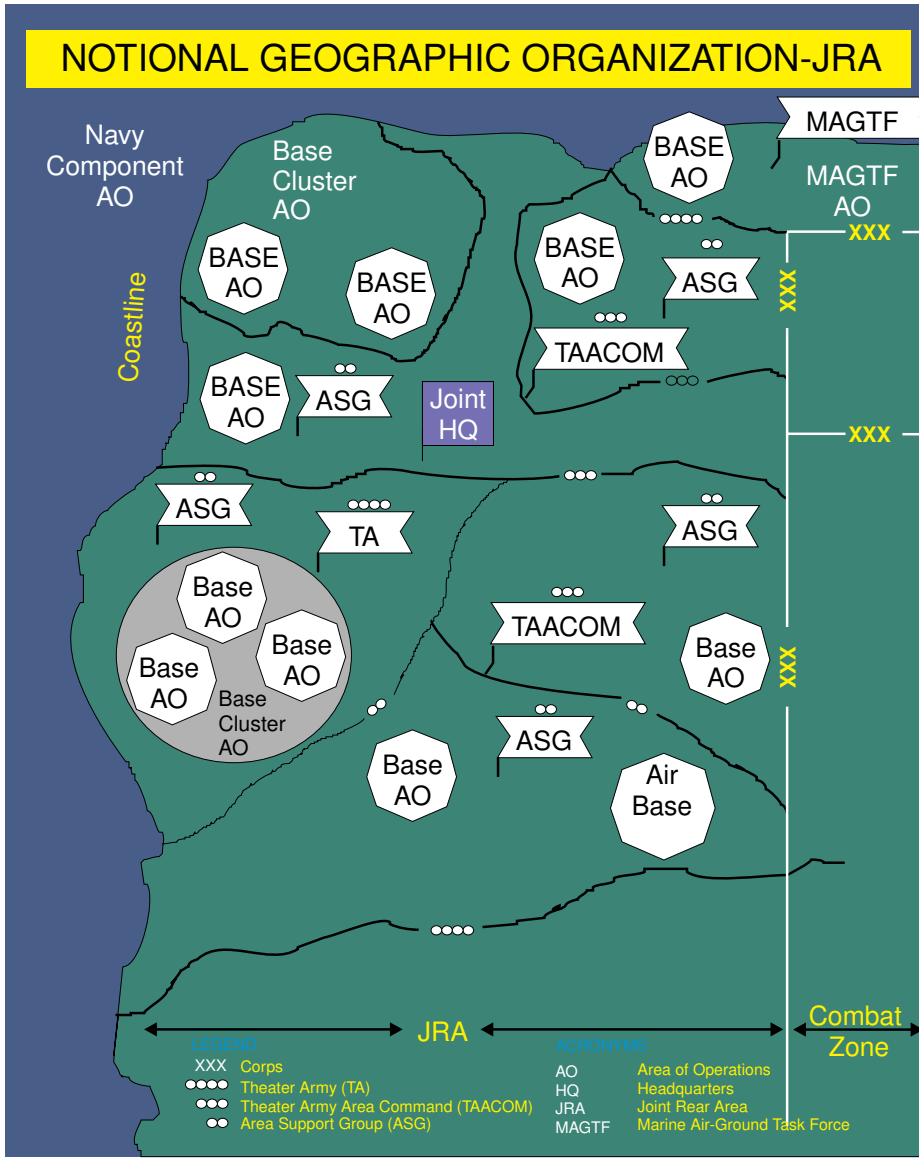


Figure II-3. Notional Geographic Organization—JRA

commanders plan, coordinate, control, and execute rear security operations through rear area operations centers (RAOCs) or rear tactical operations centers (RTOCs) (see subparagraph 1b).

- **The JRA (or a part of the JRA) may be the responsibility of the Commander, Marine Forces (COMMARFOR).** The COMMARFOR may designate to the commander of the Marine air-ground task force (MAGTF) the mission of Marine Corps rear area operations, including the defense of logistic and air bases. The MAGTF commander may, in turn, choose to designate the MAGTF combat service support commander for this mission.

g. **Base Cluster Commanders.** The base cluster commander (base community commander assumes this responsibility in selected theaters), when designated, **is responsible for coordinating the defense of bases within the base cluster and integrating base defense plans into both a base cluster defense plan and the area defense plan**. Specific responsibilities for base cluster defense include:

- Establishing a base cluster operations center (BCOC) from available base or cluster assets to serve as the focal point for security operations in the base cluster area of operations and integrate execution of local base defense plans with the next echelon RAOC or RTOC (See subparagraph 3c); and

- Providing appropriate facilities and housing for necessary liaison personnel from bases within the cluster.

Integral to the rear area security plan is the operation of base defense faciltiies.

h. **Base Commanders.** Base commanders (or senior installation commanders) **are responsible for the defense of their bases**. The forces of other Service components assigned to the base for base defense will be under the base commander's operational control (OPCON). Forces of other Service components assigned or attached to the base for purposes other than base defense will support the base defense effort during an attack or threat of an attack. The base commander's **specific responsibilities** for defense of the base include the following.

- **To establish a base defense operations center (BDOC) and an alternate BDOC** to serve as the focal point for security operations in the base defense area of operations and integrate execution of local base defense plans with the next echelon RAOC or RTOC. (See subparagraph 3d.)

- **To plan for employment of transient forces** by ensuring that base defense plans include provisions for augmenting the regularly assigned base defense forces during an attack or when the base is threatened with attack. **In an emergency, the base commander will be considered to be an area commander.** As such, the commander will have the authority to require support from transient forces for base defense. Principles governing support provided by a transient force during an emergency, and the responsibilities of the commanders concerned, are fully addressed in Joint Pub 0-2, "Unified Action Armed Forces (UNAAF)."

- **To maintain liaison with adjacent bases, base clusters and supporting HN security agencies.** Responsibilities for liaison may be retained by higher authority or delegated to subordinate commands as local circumstances dictate.

- **To develop base defense plans** that incorporate tenant units.

- **To disseminate air, ground, and missile attack warnings** using established warning alarms.
- **To maintain communications with the designated reinforcing and tactical combat forces.**
- **To integrate area security plans** with the RAOC and RTOC.
- **To maintain communications with supporting emergency ordnance disposal unit.**
- **To develop and request information requirements** to support area defense operations.

i. **Tenant Unit Commanders.** The commanders of tenant forces at a base are responsible for the items shown in Figure II-4.

j. **Response Force Commanders.** The response force is **a mobile force designated, usually by the area commander, to deal with Level II threats**. Response force commanders may be put under the tactical

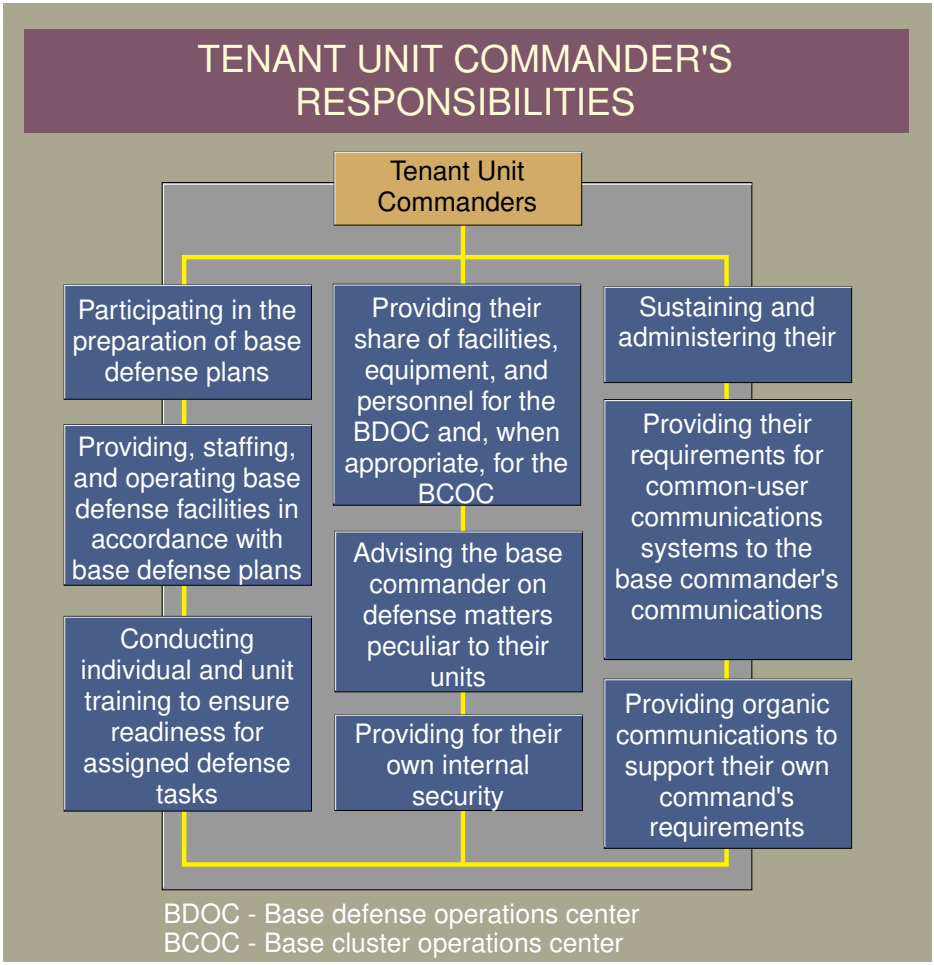

TENANT UNIT COMMANDER'S RESPONSIBILITIES
Tenant Unit Commanders
Participating in the preparation of base defense plans
Providing, staffing, and operating base defense facilities in accordance with base defense plans
Conducting individual and unit training to ensure readiness for assigned defense tasks
Providing their share of facilities, equipment, and personnel for the BDOC and, when appropriate, for the BCOC
Advising the base commander on defense matters peculiar to their units
Providing for their own internal security
Sustaining and administering their
Providing their requirements for common-user communications systems to the base commander's communications
Providing organic communications to support their own command's requirements
BDOC - Base defense operations center
BCOC - Base cluster operations center

Figure II-4. Tenant Unit Commander's Responsibilities

control (TACON) of commanders of threatened bases. They may be assigned their own AOs, where they will coordinate with base defense forces within the AO under a common superior. Every opportunity should be taken to plan and rehearse response force operations within the AO.

k. **Tactical Combat Force Commanders. The TCF commander is designated by the JFC.** The command relationships between the TCF and the JRAC or commanders in the JRA will be determined by the JFC. **The TCF is a combat unit, with appropriate combat support and combat service support assets, which is assigned the mission of defeating Level III threats.** The threat requiring the commitment of a TCF is usually of such magnitude that several bases or base clusters are threatened. The TCF commander may be directly subordinate to the JFC or to a component commander. Once committed, the TCF is given an AO in which to accomplish its assigned mission. Plans for the employment of the TCF should be coordinated with component commanders, area commanders, base cluster commanders, base commanders and with the HN. The TCF and base defense forces should conduct training exercises and rehearsals to ensure that C2 procedures are effective. Joint Pub 3-10, "Doctrine for Joint Rear Area Operations," discusses TCFs in detail.

3. Operations Centers

a. **Joint Rear Tactical Operations Center. The JRAC will establish a joint rear tactical operations center (JRTOC), using joint force staff elements and representatives from components operating in the JRA** to assist in meeting JRA security responsibilities. Component and staff representation will vary in accordance with mission, forces, and area requirements, and should support the planning, coordination, and execution of JRA operations. The JRAC will ensure that component representation and representation from the JRAC staff is sufficient to support assigned mission responsibilities. The JRTOC should be collocated with a RAOC or RTOC where possible. The JRTOC serves as the JRAC's centralized planning, coordinating, monitoring, advising, and directing agency for JRA operations. It coordinates with other

The Tactical Combat Force operates within an assigned area of operations to accomplish their mission.

elements on the JRAC staff, with higher, lower, and adjacent command staffs, and with HN and allied command staffs.

b. **Rear Area Operations Centers and Rear Tactical Operations Centers. Army and Marine Corps area and subarea commanders usually have RAOCs and RTOCs** to assist in accomplishing their base defense missions. These C2 facilities serve as the area and subarea commanders' planning, coordinating, monitoring, advising, and directing agencies for area security operations.

c. **Base Cluster Operations Centers. The base cluster commander establishes a BCOC** from available base or cluster assets to serve as the focal point for defense operations. Its functions are similar to those of individual BDOCs, and it also may serve as the BDOC for the base on which it is located.

d. **Base Defense Operations Centers. The commander of the base establishes a BDOC from available base assets.** It serves as the focal point for base security and defense. The BDOC frees the base staff to concentrate on primary support missions. The BDOC may be composed of elements of the base commander's headquarters, elements from tenant units, or a combination of both. **The BDOC plans, directs, integrates, coordinates, and controls all base defense efforts** and coordinates and integrates into area security operations with the RAOC and RTOC. For the purposes of this publication, **the BDOC performs three critical functions: operations, intelligence (including CI), and communications**. Some functions, especially on Air Force installations, may be performed by other base command facilities. Appendix D, "Base Defense Operations Center," sets forth the organization of a notional BDOC and a discussion of Air Force base organization.

- **Operations.** The operations section is **primarily concerned with planning and coordinating current and potential defense operations**. It prepares and implements base security and defense plans and serves as the central point of contact for coordination with:
  - Higher echelon area defense counterparts;
  - Other bases;
  - Area MP forces;
  - Tactical combat forces and response forces;
  - HNS forces;
  - Area damage control (ADC) teams;
  - Fire support units; and
  - Close air support units.
- **Intelligence and Counterintelligence.** The intelligence section is **the base commander's focal point for threat analysis**. It also transmits pertinent intelligence information. It develops or requests information from the sources shown in Figure II-5.
- **Communications. Dedicated communications assets should link all base defense activities and interface with higher echelons.** The communications system should have antijam characteristics, provide transmission security, and be robust, redundant, and reliable. It should interface with the communication systems of HN and US response forces. See Chapter III, "Communications."

INTELLIGENCE AND COUNTERINTELLIGENCE SOURCES OF INFORMATION
• Supporting host-nation and US civil or military intelligence and security agencies and units
• Area security patrols
• Convoys
• Adjacent bases
• Communications sites
• Higher echelon sources
• Movement control
• Medical evacuation assets
• Defector and enemy prisoner of war

Figure II-5. Intelligence and Counterintelligence Sources of Information

e. **Alternate BDOCs and BCOCs.** For reliable, survivable C2, **base commanders should set up alternate BDOCs and BCOCs if possible**. If bases do not have the resources to support this requirement, headquarters elements of units OPCON to bases for defense may be designated for this purpose. C4 connectivity should be the main factors in selecting locations of the alternate BDOCs and BCOCs.

4. Assigned Areas of Operations

The assignment of AOs to commanders is key to the C2 of JRA defense. Just as boundaries and other control measures in the combat zone identify the zones and sectors that are the responsibilities of tactical commanders, **AOs in the JRA both fix and limit the geographical defense authority for commanders in the JRA**. The JRAC should provide recommended AOs to the JFC for component and area commanders whose boundaries include all critical areas in the JRA. Component and area commanders, in turn, must ensure that AOs assigned to base and base cluster commanders encompass all territory necessary to conduct effective defense operations. **Special attention must be paid by all commanders to AO boundaries.** Command arrangements within each AO must be clearly established for all anticipated situations, especially when forces of different joint force components and nations occupy the same AO.

5. Liaison

Intelligence and operations liaison within and between bases, base clusters and higher headquarters is essential in developing defense plans and executing defensive operations. Early and continuous liaison with HN and allied organizations, and with established response forces, must be conducted to ensure effective and coordinated actions when required.

6. Nonmilitary Agencies

a. **Commanders must establish C2 measures to integrate the defensive capabilities and defense requirements of civilian agencies of the US and HN governments.** Private contractors also may

ARAB-ISRAELI CONFLICT

The Arab air forces were a significant threat to their enemy, Israel. The Israelis clearly recognized this. In World War II, future Israeli commanders learned well from the RAF. Later, in 1956, they saw again what air power did to Egypt's Air Force. The 1967 attack on the EAF was a direct outgrowth of the French-British success at neutralizing the Egyptians during the Suez Crisis. Geography, which limited the number of Israeli airfields, combined with a sense of desperation among IAF commanders to promote a belief in the necessity for a first strike. Lacking the political limitations the Americans accepted in Southeast Asia, the Israelis were more aggressive in planning and weapon development. The resulting low level attacks of June 5, 1967, destroyed for a time the Arabs' air capability. The shock to Arab pride was great, but it did not preclude their devising better ways to protect airplanes.

In the 1967 conflict, the Israelis' sudden strike, including the use of special "concrete dibber bombs," left the EAF paralyzed. Aircraft losses were heavy, and runway damage repair was slow. Some bases were out of operation for long periods. This was not the case in October 1973 when adequate advance preparation of hardened structures protected most aircraft, and expertly trained repair crews restored bases to use in hours. Protected aircraft parking areas and other facilities (such as ammunition dumps, fuel storage, and power generation units) increased the difficulty of destroying an air base. When the Israelis struck at Egyptian and Syrian bases in 1973 and found they had no weapon to penetrate hardened hangarettes, they realized what the *Luftwaffe* learned at Malta in 1942, and before that over England in 1940: successful attacks on bases required proper weapons to overcome the passive as well as the active protective measures encountered.

SOURCE: John F. Kries, Air Warfare and Air Base Defense
Office of Air Force History, 1988

require security. Defense-related resources of these agencies may include police, fire departments, private security guards, observers, and mechanical or electrical security systems. Integration may be accomplished by memorandums of understanding or similar instruments that set forth the requirements and capabilities of all participating organizations.

b. **Nonmilitary agencies may have communications networks established for their uses.** These networks may include commercial leased circuits, commercial-based satellite services (such as International Maritime Satellite Organization), and high frequency and very high frequency radios.

c. Civilian organizations and other agencies **may want to use military communications assets** once they are established. Commanders may need to establish a policy concerning this use.

d. Commanders should **address the need for secure communications and requirements to control cryptographic materials**. A policy for the release of classified communications information should be introduced early in the operation.

e. **Spectrum Management.** Frequency management must be identified and planned. Commanders should ensure that they account for frequencies already in use by nongovernmental

organizations, private voluntary organizations, UN agencies, HN agencies, religious organizations, and other organizations involved in the operational area.

f. Further information on nonmilitary agencies may be located in Joint Pub 3-08, "Interagency Coordination During Joint Operations."

CHAPTER III
COMMUNICATIONS

"Co-equal with the security of flanks, the maintenance and full use of the line of communications to the rear are of major concern to the commander. It is his responsibility that the incoming supply is equal to the needs of his deployments and that the supporting arms and fires which have been promised him keep their engagements. Or if they do not, he must raise hell about it."

Brigadier General S.L.A. Marshall
Men Against Fire, 1947

1. General

Effective communications for joint base defense present numerous challenges. All component communications systems on the base, both secure and unsecure, must be compatible in order to facilitate effective C2 of defense and security operations. **The BDOC, as the focal point for base defense C2, is normally the hub for the base defense communications system.**

2. Planning and Construction Considerations

Base communications facilities for both defense and primary missions must be planned, coordinated, and established. **The joint agency responsible for planning base defense communications will depend on the mission.** The base Communications Electronics Officer for a single-Service garrison mission or the C4 staff officer (J-6) for a Marine Corps- or Army-lead joint mission are options for this responsibility. Considerations include the following.

a. Organization and integration of capabilities and resources.

b. Specific procedures for transitioning from a permissive operating environment to an uncertain or hostile environment.

c. Communication system redundancy or equivalent backup systems.

d. Compatibility of equipment and systems.

e. Selection, preparation, and hardening of communications installations.

f. Determination of requirements for on-call augmentation from off-base communications assets.

g. Requirements for control of air support and fire support.

h. Ability to operate in an electronic warfare (EW) environment.

i. Secure voice and data communications.

j. Transmission security and communications deception.

k. Development of signal operating instructions or communications plans and dissemination to tenant, supporting, and augmentee units. Communications plans should be integrated into the JFC's Joint Communications Electronic Operating Instructions to ensure deconfliction of frequencies and call signs.

l. Coordination with HN, TCF, and transient units.

3. Capabilities

a. **Existing base communications facilities are used to the maximum extent possible for base defense.** However, if such use would divert communications resources from support of the primary base mission, a separate communications system may be necessary. **Wire is the normal means of internal base communications between fixed sites** like sentry posts, checkpoints, and the BDOC. **When dealing with Level II and Level III threats, radio will become the primary carrier for tactical traffic.**

b. **Plans should be developed to provide for alternate means of communications.** Planners should also consider the possibility of using community communications systems, such as base cable, armed forces, or civilian-owned radio broadcast stations and television. PSYOP capabilities should be considered when planning for alternate means of communications.

c. **The base mission operations center and BDOC should net with theater warning systems** so that timely action may be taken against NBC, air, missile, and ground attacks. Alarms using loudspeakers, sirens, pyrotechnics, or other established methods (metal banging metal) should be used to sound warnings of those threats. Complete knowledge of the alarm system by all base personnel and rehearsals of required actions are critical to the system's effectiveness.

4. Base Defense Communications System

A secure, robust, redundant, reliable communications system is required between defense units, staff elements, headquarters, and operations centers. A communications system can be enhanced by using automated systems, voice combat nets, and trunked land mobile radios. It should include, if equipment permits, the items shown in Figure III-1.

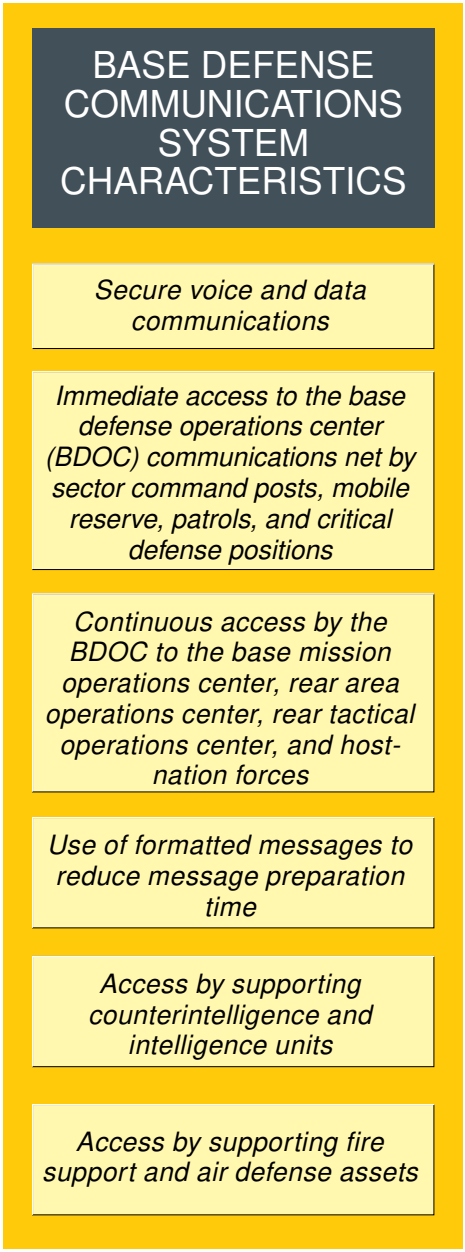

BASE DEFENSE COMMUNICATIONS SYSTEM CHARACTERISTICS
Secure voice and data communications
Immediate access to the base defense operations center (BDOC) communications net by sector command posts, mobile reserve, patrols, and critical defense positions
Continuous access by the BDOC to the base mission operations center, rear area operations center, rear tactical operations center, and host-nation forces
Use of formatted messages to reduce message preparation time
Access by supporting counterintelligence and intelligence units
Access by supporting fire support and air defense assets

Figure III-1. Base Defense Communications System Characteristics

5. Base Defense Communications Nets

Figure III-2 is a notional structure for base defense communications. The following units or facilities should operate stations in the base defense net.

a. Base Operations Center and other C2 facilities such as those found on Air Force installations.

b. BDOC.

c. Fire support element (FSE) or Fire Support Coordination Center (FSCC).

d. Defensive sector command post.

e. Base observation posts (OPs), listening posts (LPs), and patrols.

f. Base mobile reserve.

g. Theater air control system.

h. BCOC.

i. NBC air defense and missile warning.

j. Maritime and offshore defense forces.

k. RAOC and RTOC.

l. Response force and TCF.

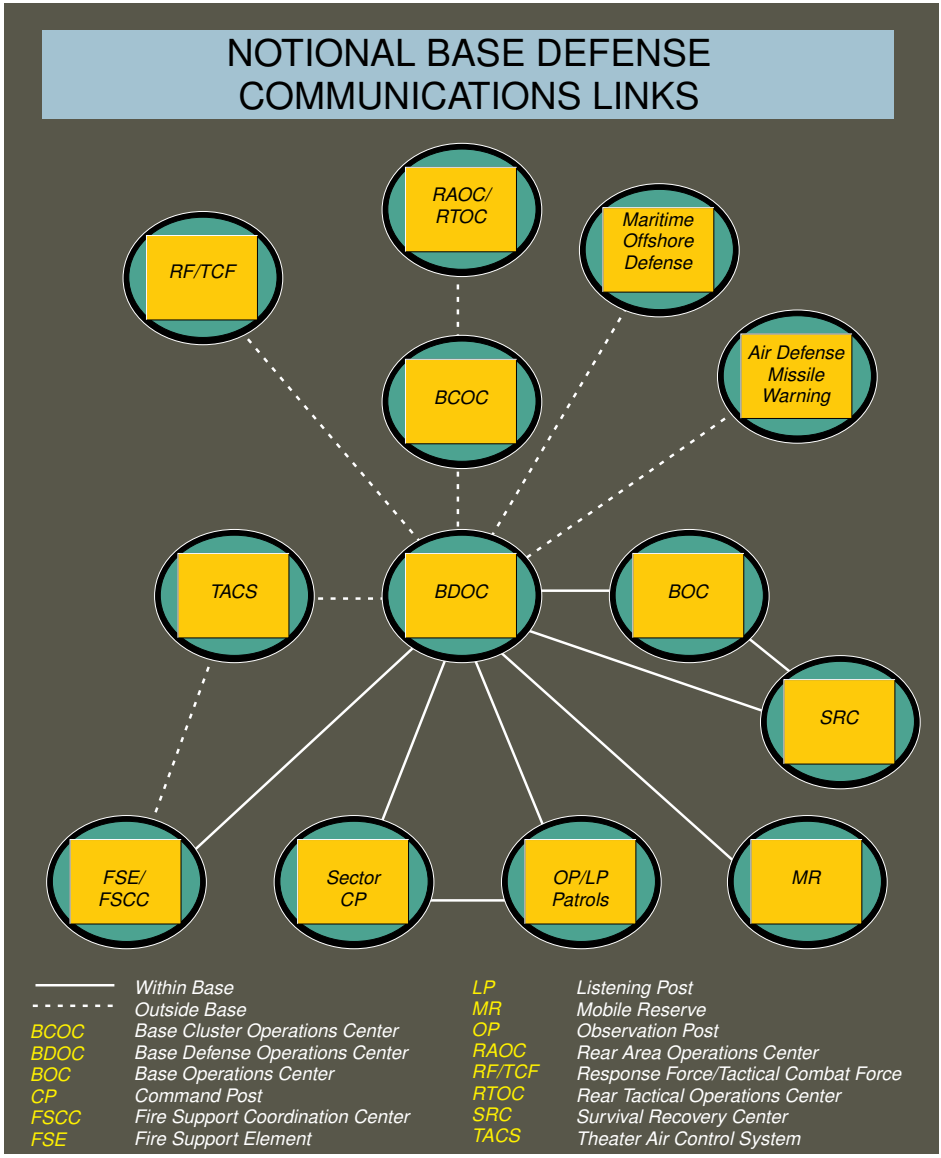


Figure III-2. Notional Base Defense Communications Links

CHAPTER IV
BASE DEFENSE OPERATIONS

"He passes through life most securely who has least reason to reproach himself with complaisance toward his enemies."

Thucydides
History of the Peloponnesian Wars, I, 404 BC

1. General

The base commander organizes and controls all forces assigned to the base to capitalize on their capabilities. These forces must be trained, organized, and equipped to contribute to the defense of the base. This chapter sets forth the factors that the base commander must consider in preparing and executing defense plans. A format for a sample base defense plan is in Appendix E, "Sample Base Defense Plan."

2. The Fundamentals of Base Defense

The general characteristics of defensive operations are discussed in detail in Service doctrinal publications. **Defensive fundamentals**, as they pertain to the defense of bases, are shown in Figure IV-1 and are as follows.

a. **Understand the Enemy.** Defenders must **be familiar with the capabilities and**

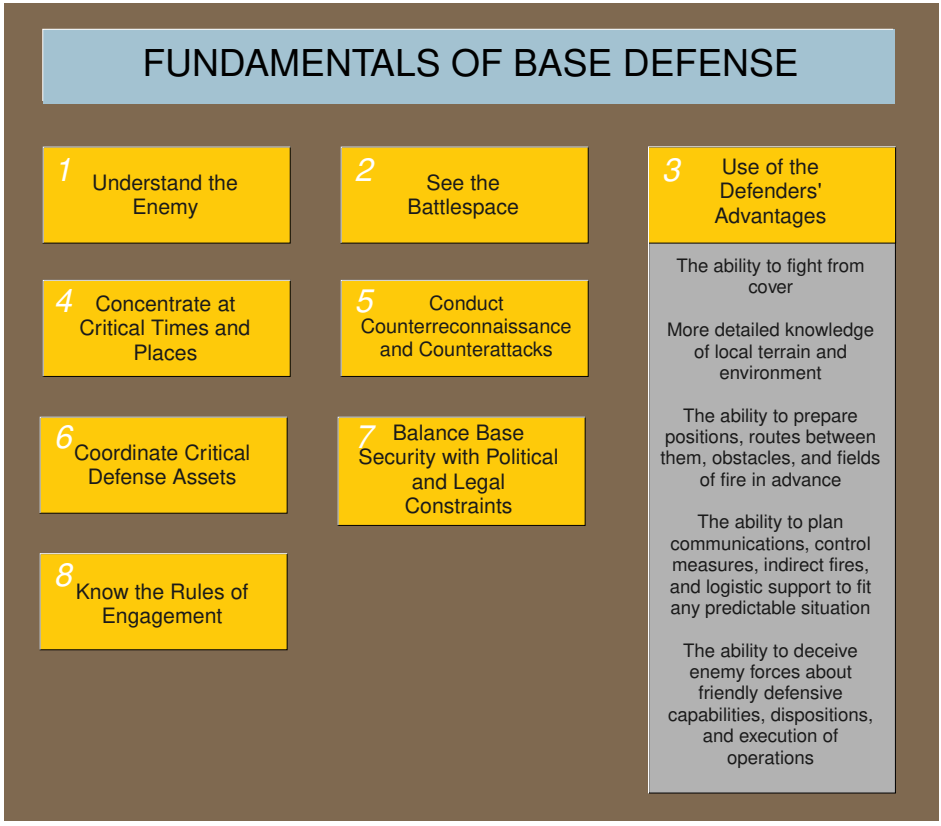

FUNDAMENTALS OF BASE DEFENSE
1 Understand the Enemy
2 See the Battlespace
3 Use of the Defenders' Advantages
The ability to fight from cover
More detailed knowledge of local terrain and environment
The ability to prepare positions, routes between them, obstacles, and fields of fire in advance
The ability to plan communications, control measures, indirect fires, and logistic support to fit any predictable situation
The ability to deceive enemy forces about friendly defensive capabilities, dispositions, and execution of operations
4 Concentrate at Critical Times and Places
5 Conduct Counterreconnaissance and Counterattacks
6 Coordinate Critical Defense Assets
7 Balance Base Security with Political and Legal Constraints
8 Know the Rules of Engagement

Figure IV-1. Fundamentals of Base Defense

limitations of enemy forces, weapons, equipment, and tactics. The base commander also must have access to the latest intelligence concerning probable enemy intent.

b. **See the Battlespace.** Intelligence operations are key to assembling an accurate picture of the battlespace. The **intelligence preparation of the battlespace provides the commander a continuous, integrated, and comprehensive analysis of the effects of enemy capabilities, terrain, and weather on operations**. It helps the commander anticipate battlespace events and develop the priority intelligence requirements (PIR) and information requirements tied to those battlespace events. Intelligence and multidiscipline CI estimates are prepared, continuously updated, and integrated into the base commander's staff decision making process.

- The ability to fight from cover;
- More detailed knowledge of local terrain and environment;
- The ability to prepare positions, routes between them, obstacles, and fields of fire in advance;
- The ability to plan communications, control measures, indirect fires, and logistic support to fit any predictable situation; and
- The ability to deceive enemy forces about friendly defensive capabilities, dispositions, and execution of operations.

Base commanders use appropriate assets made available to conduct intelligence operations and gain an accurate picture of the battlespace.

c. **Use of the Defenders' Advantages. Defenders' advantages may permit a numerically inferior force to defeat a much larger one.** Some of these advantages are:

d. **Concentrate at Critical Times and Places. Defense of a base is normally conducted along interior lines, permitting the timely and secure movement of forces to engage the most critical threats.** The commander must mass enough combat power at points of decision by economizing in some areas, employing a reserve, and maneuvering to gain local superiority at critical points.

e. **Conduct Counterreconnaissance and Counterattacks.** Fixed bases having well-established perimeters usually have limited depth. **Counterreconnaissance and counterattack add depth to the battle** outside the perimeter, allowing the base to continue its primary mission with minimal interference.

f. **Coordinate Critical Defense Assets.** Synchronization of indirect fires, air and missile defense resources, tactical aircraft, engineers, dismounted troops, armored vehicles, naval surface fire support, and helicopters can produce a combined arms effect. **Synchronizing forces and fires produces a synergy capable of defeating a larger enemy force.** This synergy results from making enemy movement difficult or impossible and by causing a reaction that may make enemy forces more vulnerable to other friendly capabilities.

g. **Balance Base Security With Political and Legal Constraints.** Base security may have to be designed around numerous political constraints.

h. **Know the Rules of Engagement.** Base commanders and their subordinates must comply with ROE. They should ensure that inconsistencies among Service component ROE are reconciled.

3. Defensive Factors

The remainder of this chapter deals with base defense against action by organized military or paramilitary units. Considerations for day-to-day security of the base and for combatting terrorism are contained in Appendix F, "Security," and Appendix G, "Terrorism." As shown in Figure IV-2, **base defense should be governed by considering the factors of mission, enemy, terrain and weather, troops and support available, and time available** (including all friendly forces). Additionally, careful consideration should be given to the protection of any key strategic or operational assets located at a base.

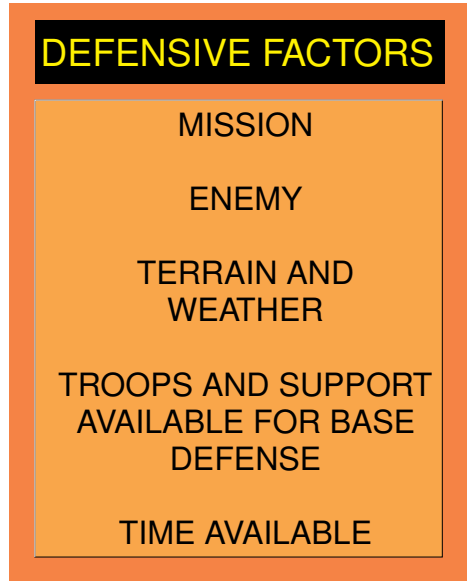


Figure IV-2. Defensive Factors

a. **Mission. The primary mission of the base is to support joint force objectives.** Inherent in this mission is the subsidiary mission of defending itself.

- The stated defense plan should specify the following essential elements.
  - •• Who will defend the base.
  - •• Where each unit will defend.
  - •• When and for how long the unit must be prepared to defend.
  - •• Why the unit will defend.
  - •• What the unit will defend.
- **Essential actions of the defense force are:**
  - •• **Detect** -- Enemy attempts to reconnoiter or attack the base or interfere with the performance of base functions

must be detected at the earliest stage possible;

•• **Warn** -- The base must be warned that an attack is imminent or under way;

•• **Deny** -- Defense forces must prevent the enemy from access to the base and from degrading the base's primary function;

•• **Destroy** -- If possible, defense forces must eliminate the attacking enemy's capability to threaten the base; and

•• **Delay** -- If base forces lack the combat power to defeat the attacking enemy, defense forces must disrupt the attack and attempt to create the conditions for response forces or tactical combat forces to react and destroy the enemy force or to remove or deny base resources to the enemy.

b. **Enemy.** Every intelligence and counterintelligence resource available to the base commander should be used to **determine enemy capabilities and intentions**. The intelligence cycle and intelligence support to joint operations are discussed in Joint Pub 2-0, "Joint Doctrine for Intelligence Support to Operations."

- **Priority intelligence requirements** are the means by which the commander provides direction for intelligence operations. The answers to questions raised by PIR will indicate or confirm particular enemy courses of action. **PIR may include:**

  •• The enemy's tactical, operational, and strategic objectives and intentions;

  •• Organization, size, and composition of forces, and locations of their strongholds;

  •• Movement of personnel and equipment;

  •• Religious, political, or ethnic affiliation;

  •• Enemy intelligence capabilities;

  •• Tactics, operational procedures, and patterns of operations;

  •• Special skills (e.g., sniping, demolitions, sabotage);

  •• Motivation, morale, discipline, and fanaticism;

  •• International support;

  •• Support among HN population;

  •• Identities and psychological characteristics of leaders;

  •• Logistic capabilities and patterns of activities to prepare for operations; and

  •• Medical capabilities and evacuation support.

- **Information requirements** deal with information about an enemy and the environment that needs to be collected and processed in order to meet the intelligence requirements of the commander.

- The intelligence effort should be directed toward collection, exploitation, analysis, and dissemination of intelligence that will permit the development of friendly capabilities to:

  •• Identify and counter enemy operations security (OPSEC) measures, deceptions, PSYOP, and attacks;

•• Counter enemy firepower, mobility, EW, imagery, and human intelligence (HUMINT) capabilities;

•• Destroy, exploit, and/or neutralize enemy strengths;

•• Exploit enemy vulnerabilities; and

•• Identify and defend against enemy security and counterintelligence capabilities.

c. **Terrain and Weather. Sites for bases are usually selected in order to accomplish assigned primary missions.** Although defensive considerations are frequently secondary, they must not be ignored. The nature of air bases, for example, precludes establishment of a tight perimeter with extensive cover and concealment for defenders. However, the location of an air base could be chosen to make defense easier by making an unobserved enemy approach more difficult. Likewise, the best ports are located in or adjacent to urban areas. **Nonetheless, the base commander must make the best use of the terrain within the commander's AO.** Commanders analyzing terrain must consider all its military aspects, from the standpoints of both defenders and the enemy. These include observation and fields of fire, cover and concealment, obstacles, key terrain, and avenues of approach. Additionally, commanders must analyze the effects of weather on both defender and enemy weapons systems and tactics. **Weather and visibility conditions can have significant effects on ground, air, and maritime operations.** Commanders should minimize their own vulnerabilities to adverse weather conditions and exploit any advantages over enemy vulnerabilities.

d. **Troops Available for Base Defense.** There may be some units on a base whose missions are defense and security, such as MPs at a large headquarters, security police (SPs) on an air base, and air defense forces. However, **most of the personnel available for defense (augmentees and selectively armed personnel) will be obtained from the units devoted to the accomplishment of the base's primary mission**. These personnel will not have the same degree of combat skills as dedicated security forces, and therefore

When possible, defensive positions should be selected that make an unobserved enemy approach difficult.

must receive regular training in marksmanship, tactics, and basic ground combat skills. Their contribution to a successful base defense will require close supervision and leadership. Service doctrinal and training publications discuss the needed skills and standards to be attained. The task organization of the base defense plan should take into account the personnel available and the weapons and equipment organic to their units, so that all available combat power on the base may be brought to bear in the event of hostile action. An analysis of the threat may show the necessity of tasking combat forces for a rear area mission when attack in the rear area seems probable.

- **Defending Against Level I Threats.** At this level, **available base assets should be able to detect and defeat enemy activities**. Day-to-day security activities are conducted by the forces assigned to the base, usually as tasks in addition to their primary duties. At Level I, base defense forces must be trained and exercised to permit smooth transitions to Level II and Level III.

- **Defending Against Level II and Level III Threats.** After transition from a Level I posture to a posture able to engage Level II and Level III threats, **base defense forces must be able to disrupt or delay hostile action until response forces or TCF can be committed**.

- **Evaluating the Defense.** Commanders of bases must evaluate and plan to:

  •• Use indirect fires to maximum advantage;

  •• Use organic and supporting direct fire weapons to maximum advantage;

  •• Patrol the base AO;

  •• Use available air and missile defense capabilities;

  •• Use the mobility of its own combat and combat support elements;

  •• Use engineers in countermobility and survivability roles;

  •• Constitute a reserve, plan for its use, and rehearse its employment in reinforcement, blocking, and counterattacks;

  •• Sustain the defense forces themselves and continue the support of the larger force;

  •• Avoid, detect, protect from, react to, and recover from NBC attacks;

  •• Employ OPSEC measures and deceptions;

  •• Maintain surveillance of beaches, concealed water approaches (e.g., bayous and swamps), and rivers;

  •• Maximize rail and highway entrance security; and

  •• Use PSYOP personnel.

e. **Time Available.** Base commanders will set priorities of work to make best use of the time available to plan, prepare, train for, and evaluate the defense.

4. Base Commander's Intelligence Responsibilities

The base commander is responsible for ensuring that **the following intelligence functions are performed in a timely manner**.

a. **Provision of information and intelligence to the defense force** and maintaining current threat data bases.

b. **Establishment of intelligence liaison** with applicable area, subarea, higher, and

adjacent commands, including the joint force joint intelligence center or joint intelligence support element, HN and third country military intelligence facilities, and US and HN civilian organizations.

c. **Direction of the reconnaissance and observation effort** of the base defense force and arrangement for reconnaissance and observation, to be conducted by commands supporting the base defense force. Deconfliction of these intelligence collection efforts is an ongoing process in which the base commander and the intelligence staff must take part.

d. **Collection of target information** and the dissemination of this information to base cluster or other higher headquarters, the FSE or FSCC (if provided) and any units providing fire support to the base.

e. **Procurement** of nonstandard maps, charts, and imagery.

f. **Development and implementation** of local CI measures.

g. **Request for augmentation or support** by intelligence specialists.

h. **Establishment and maintenance of contact** with local HN police and intelligence agencies.

5. Planning

Base commanders develop defense plans (Appendix E, "Sample Base Defense Plan") to use in organizing base defenses.

a. **Forces in Base Defense Areas. Successful defense depends on integrated aggressive, all-around, in-depth measures.** Drawing from the units assigned to the base, base commanders organize defense forces within their AOs, using existing chains of command.

- **Areas of Operations. Areas within the base should be assigned to cover all likely avenues of approach and other key terrain.** Boundaries between sectors assigned to subordinate units should be well-defined, with coordinating points, contact points, and fire control measures. Fire support coordination measures are essential for subordinate tenant units to perform their AO security missions. These measures decrease the likelihood of fratricide, prevent noncombatant casualties, and minimize damage to the property of friendly civilians.

- **Defense in Depth**

  •• **A security area from the defense force's primary defense positions outward to the limits of the base AO may contain OPs, LPs, and mounted and dismounted patrols.** Defense forces in this area should be equipped with sensors and devices for periods of limited visibility as well as reliable mobile communications. Aviation support may be requested to augment the capabilities of base security forces. Contact points will be established on or near base AO boundaries, where the patrols and security forces of the area commander, HN, or adjacent bases can contact base defense forces.

  •• **Boundary areas of various base defense forces must be clearly defined, and that information be disseminated to defending forces.** Contact and identification procedures must be standardized and clearly understood by all defending forces. This can be especially critical when HN and third world country forces whose primary language is not English and US forces come into contact with each other, or when base defense forces are acting only as augmentation forces.

•• **Defense forces in the base's primary defense positions must be prepared to prevent hostile forces from penetrating the base and interfering with its primary mission.** If not capable of defeating enemy threats, the primary defense forces must fix or delay the enemy until commitment of response forces or the TCF or the removal or denial of critical resources to the enemy.

•• **Some forces** (augmentees and selectively armed personnel) **may be directed to secure areas or facilities within the base vital to performance of the base's mission.** Examples are the BDOC, ammunition storage areas, and aircraft revetments. Defensive forces deployed inside the base perimeter require careful fire control to prevent fratricide.

- **Relationship With Other JRA Defense Forces.** Upon notification by a base or base cluster commander through the BDOC or BCOC that a threat exceeds a base's defense capabilities, **the area commander, through the RAOC, commits the response forces available or requests the commitment of a TCF**. The situation will dictate the C2 relationship between the response force or TCF and the base defense force as well as whether planned arrangements should be modified.

•• If base defense forces are already engaging threat forces, the area commander normally transfers the response force to the TACON of the base commander until the threat is defeated (see Figure IV-3).

•• When response forces are committed before the base defense forces are engaged, the area commander normally assigns the response force a AO close to or contiguous to the base AO (see Figure IV-4). The base commander may transfer selected base defense forces to the TACON of the response force commander.

•• **When a TCF is committed, the situation is serious enough to assign to the TCF commander a AO that encompasses a large portion of the rear area.** During Level III operations, the TCF commander will normally have OPCON over most base or base cluster defense forces and response forces in the assigned AO, excluding air defense forces, which remain under OPCON of the AADC. Some base defense forces necessary for the protection of critical base assets may remain under the control of the base commander. BDOCs and/or BCOCs will establish and maintain contact with the tactical operations center of the TCF (see Figure IV-5).

b. **Mobile Reserve. The base's mobile reserve** may be used to reinforce threatened areas of the base perimeter, to block enemy penetrations of primary defense positions, or to counterattack in order to regain lost defense positions or destroy the hostile attacking force. **It should be vehicle-mounted, in armored vehicles if available.** On large bases or base clusters, the reserve may be airmobile if helicopters are available.

c. **Antiarmor Weapons. Rear area forces generally have few organic antiarmor weapons.** Antiarmor weapons, including tanks, available to base defense forces will be positioned to cover the most likely high-speed avenues of enemy vehicular approach in mutually supporting positions. Crews must select primary, alternate and supplementary positions, with covered and concealed routes between positions to maximize weapons effectiveness and survivability. Augmentation forces possessing antiarmor weapons should also

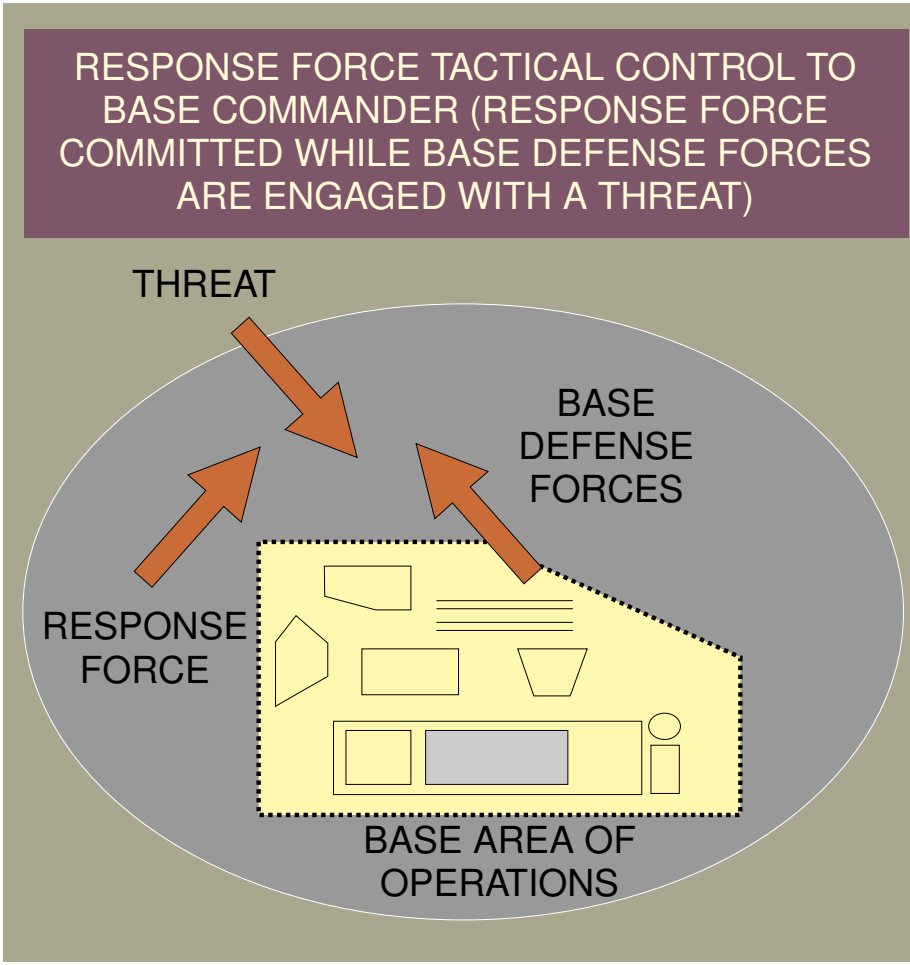

RESPONSE FORCE TACTICAL CONTROL TO BASE COMMANDER (RESPONSE FORCE COMMITTED WHILE BASE DEFENSE FORCES ARE ENGAGED WITH A THREAT)
THREAT
BASE DEFENSE FORCES
RESPONSE FORCE
BASE AREA OF OPERATIONS

Figure IV-3. Response Force Tactical Control to Base Commander (Response Force Committed While Base Defense Forces Are Engaged with a Threat)

select positions in anticipation of being committed to defend the base.

d. **Indirect Fire Systems.** The fires of mortars, field artillery, and naval guns can support the base defense effort.

- **Fire Support Planning. The FSE or FSCC of the BDOC is the focal point for the planning of fires for base defense.** If the base is too small to have its own FSE or FSCC, its BDOC operations personnel must coordinate with fire support personnel at the FSE or FSCC, at the BCOC or the appropriate RAOC. Preplanned targets should include probable landing zones (LZs) and drop zones (DZs), avenues of approach, key terrain, obstacles, final protective fires for defensive positions, and obscuration to facilitate movement of counterattack forces. The targets should be planned to minimize collateral damage and civilian casualties. Copies of fire plans and target lists must be provided to the headquarters controlling the fire support assets. Targets may be planned outside the base AO after

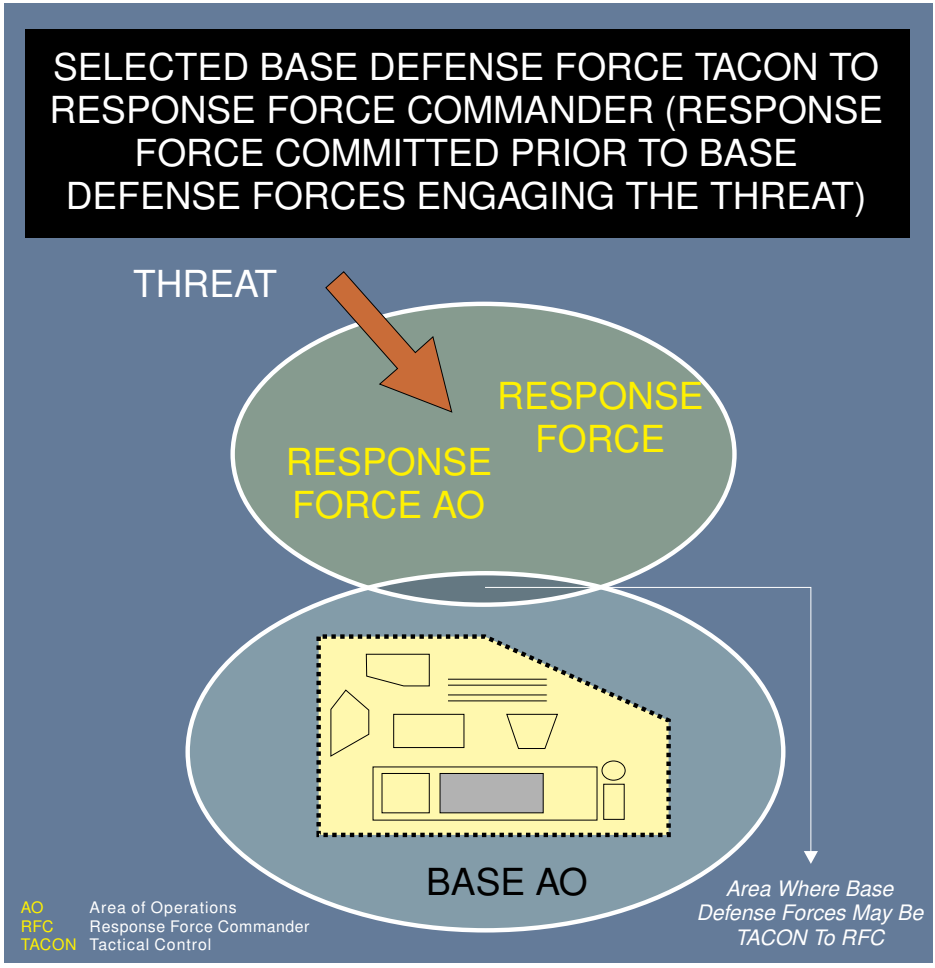

SELECTED BASE DEFENSE FORCE TACON TO RESPONSE FORCE COMMANDER (RESPONSE FORCE COMMITTED PRIOR TO BASE DEFENSE FORCES ENGAGING THE THREAT)
THREAT
RESPONSE FORCE
RESPONSE FORCE AO
BASE AO
Area Where Base Defense Forces May Be TACON To RFC
AO Area of Operations
RFC Response Force Commander
TACON Tactical Control

Figure IV-4. Selected Base Defense Force TACON to Response Force Commander (Response Force Committed Prior to Base Defense Forces Engaging the Threat)

coordination with the headquarters responsible for the area concerned.

- **Fire Support Coordination Measures.** Fire support coordination measures permit or restrict fires in and around bases. **Careful coordination must take place in planning these measures, especially with the HN.** No-fire areas may be required to protect civilians or to prevent disruption of rear area missions by friendly fire.

- **Observers.** Fire support units normally will not furnish observers to bases in the rear area. **Observers with appropriate training should be identified on each base** to adjust supporting fires and control close air support.

- **Joint Pub 3-09, "Doctrine for Joint Fire Support."** Joint aspects of fire support are discussed in Joint Pub 3-09. Service publications provide additional information on fire support planning and fire support coordination measures.

- **Aviation Fire Support. The base FSE or FSCC will maintain contact with the appropriate air control system to**

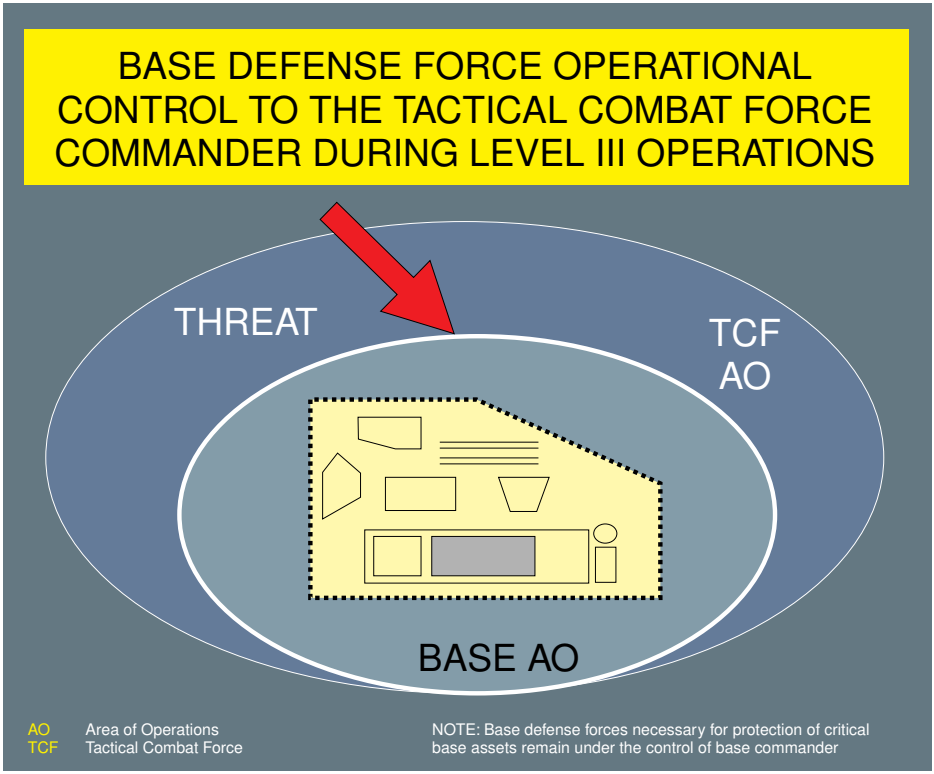

BASE DEFENSE FORCE OPERATIONAL CONTROL TO THE TACTICAL COMBAT FORCE COMMANDER DURING LEVEL III OPERATIONS
THREAT
TCF AO
BASE AO
AO Area of Operations
TCF Tactical Combat Force
NOTE: Base defense forces necessary for protection of critical base assets remain under the control of base commander

Figure IV-5. Base Defense Force Operational Control to the Tactical Combat Force Commander During Level III Operations

request and control air support for surface base defense efforts, excluding air and missile defense. When available, fixed- and rotary-wing aircraft may be used to extend the range of observation and provide immediate combat response to threats. Some aircraft, like the AC-130 gunship, are particularly well equipped to support base defense. Forward-deployed aircraft carriers can often provide a considerably effective and rapid aviation response force.

e. **Other Aviation Support. The BDOC and BCOC**, with other command and control centers, **coordinate other aspects of aviation support**. Examples include coordinating air-ground communications frequencies and procedures; coordinating time-on-target and pickup points for medical evacuation and air movement of base defense, response force, and TCF elements; and managing air support priorities and diversions for emergency resupply, personnel augmentation, and evacuation.

f. **Obstacles and Mines. Careful consideration should be given to the use of antitank and antipersonnel mines** in the rear area. However, prior to emplacement of mines or obstacles, permission must be obtained from the commander having authority over the AO in which the base is located. Often, the best avenues of enemy approach are the routes that must be used to perform base primary missions. The enemy may also transit areas of high civilian population density. Fire support plans may include the delivery of scatterable mines when enemy attack is imminent. Obstacles must be kept under observation and covered by direct and indirect fires to be effective. Some obstacles may be

useful only for certain threat levels. For example, chain-link fencing may constitute a useful obstacle against Level I threats if well-patrolled but not against higher level threats.

g. **Communications Countermeasures.** The base commander should, when capable, maintain an electronic attack and communications jamming capability to disrupt the attacking force's C2.

h. **Security Measures.** See Appendix F, "Security."

i. **Work Priorities. The commander must set priorities for the many tasks involved in base defense.** Work may occur on several concurrent tasks. Prioritizing might include the items shown in Figure IV-6.

j. **Counterattack Plans. The base mobile reserve normally conducts counterattacks** with the objective of sealing a penetration or regaining positions lost to the attacker.

k. **Area Damage Control Measures.** ADC includes the **measures taken before, during, and after hostile action or natural or accidental disasters to reduce the probability of damage and minimize its effects**. Engineers perform most of these tasks. Other forces and assets contributing to ADC include ordnance, MPs, NBC, CA, maintenance, medical, signal, supply, transportation, and transiting units, including HN units.

l. **Air and Missile Defense Measures.** Air and missile defense nullifies or reduces the effectiveness of attack or surveillance by hostile aircraft or attack by missiles after they are airborne. **Air and missile defense assets on or near a base will be integrated into the overall air and missile defense plan for the theater or joint operations area.** The base commander should establish communications links with the air defense net for early warning of impending air attack. If the base is also an air base, local air defense units and the air base operations center must coordinate identification, friend or foe (IFF) procedures. A base defense zone (BDZ) may be established around air bases with specific entry, exit, and IFF procedures. See Appendix C, "Air and Missile Defense," and Joint Pubs 3-01, "Joint Doctrine for Countering Air and

An early priority in the base defense plan may be to establish patrols outside the perimeter.

WORK PRIORITIES IN BASE DEFENSE

Identifying critical resources and preparing a base defense plan

Establishing initial base security, including observation posts and patrols outside the perimeter

Positioning crew-served weapons and troops and assigning fields of fire

Preparing and emplacing unit nuclear, biological, and chemical detection equipment

Clearing fields of fire and preparing range cards

Preparing fighting positions

Installing and hardening communications

Emplacing obstacles and mines

Hardening primary fighting positions, including overhead cover

Preparing alternate and supplementary positions

Stockpiling and hardening the locations of ammunition, food, water, and medical supplies

Preparing routes and trenches between positions

Developing a counterattack plan

Conducting rehearsals, including rehearsals of movements to supplementary and alternate positions

Figure IV-6. Work Priorities in Base Defense

Missile Threats," and 3-01.5, "Doctrine for Theater Missile Defense."

m. **NBC Defense Measures.** See Appendix B, "Nuclear, Biological, and Chemical Defense."

n. **Threat Response Contingency Plan.** The threat response contingency plan outlines specific duties and responsibilities to combat terrorism. See Appendix G, "Terrorism," and Joint Pub 3-07.2, "Joint Tactics, Techniques, and Procedures for Antiterrorism."

o. **Physical Facilities. Commanders must stress continuous upgrading for base physical security.** Activities occupying permanent fixed bases will have opportunities for installing sophisticated security equipment not available to units in mobile bases. Surveys of the defense, including intruder drills and mock attacks, must be part of defense training and serve to identify any shortcomings of base defense. **Plans for base construction must consider ADC.** Defenders must use firefighting equipment and practice procedures often to maintain proficiency. Where peacetime considerations prevent construction of defensive positions, fields of fire, and obstacles, detailed plans for their construction should be made by appropriately trained personnel. See Appendix H, "Specialized Equipment and Materiel."

- **Intrusion Detection. Defenders can place sensors on likely avenues of approach, locating them at the limits of the AO or outside the AO if coordinated with adjacent commands.** Directed ground surveillance radar and airborne forward-looking infrared systems, if available, can improve the chances of detecting intrusions early. Remotely monitored sensors, trip flares, binoculars, night vision devices and other nonlethal warning devices can also be useful. Depending on the threat situation and ROE, antipersonnel and antivehicle

CREATION OF AIR DEFENSE FORCES - WWII

German occupation of Crete in May 1941, after a rain of destruction from the air, provoked British Prime Minister Sir Winston Churchill to shoot a hotly worded memo to his secretary of state for air and to the chief of the air staff. Churchill demanded that all airmen "ought to be armed with something - a rifle, a tommy-gun, a pistol, a pike, or a mace" and trained "to fight and die in defence of their airfields; . . . every airfield should be a stronghold of fighting air-ground men, and not the abode of uniformed civilians in the prime of life protected by detachments of soldiers."

In response to Churchill's demand, the Royal Air Force Regiment, at its height 85,000 officers and men, formed in February 1942. In the same month, following Britain's example, Gen George C. Marshall, U.S. Army chief of staff, approved a similar arrangement with black troops . . . Because the Army was unwilling to place blacks in positions of responsibility, almost all of them ended up in such units as truck companies, quartermaster detachments, and "aviation squadrons,". . . The aviation squadrons . . . absorbed most of the blacks and assigned them to undefined and unskilled tasks when they were not kept busy on the drill field.

Other black units included the air base defense units, which would be responsible for "the protection of the Air Bases against riots and the possibility of parachute troops and air raids." These men were armed with rifles, 37 mm guns, and machine guns. In view if the Army's disdain for blacks at the time, assigning them to air base defense units seemed like a disparaging comment on the importance of air base ground defense. As it was, Allied control of the territory surrounding American bases made moot the need for a ground defense force. By 1943, hardly more than a year after their inception, these units faced inactivation.

SOURCE: Karl Hoover
Air Base Ground Defense: The Training Controversy, 1991

mines also may be emplaced and noncombatant use of the area restricted. Dummy sensors at observation posts and concealed surveillance resources also should be considered.

- **Observation.** To improve observation, **defenders should clear the ground to the front of positions and from near perimeter fences by cutting foliage or applying defoliant**. Because total defoliation can expose the base to aerial observation, a balance must be struck between the needs of ground defense and defense against air attack. See Joint Pub 3-11, "Joint Doctrine for Nuclear, Biological, and Chemical Defense," for a discussion of US policy on the use of herbicides. Perimeter roads on either side of the fence improve observation. A combination of concrete barriers, concertina wire, lighting, surveillance cameras, and intrusion sensors enhances base security. Figure IV-7 displays security facilities available on fixed permanent bases. Observation sites in guard towers or atop buildings can increase the surveillance capabilities of perimeter guards.

- **Communications.** Defenders should install **a reliable, secure, and redundant communications system at all guard locations**.

- **Entrances.** The base should **have as few entrances as possible**. Other measures to enhance entrance security can be found at Appendix E, "Sample Base Defense Plan," and Appendix F, "Security." Appendix H, "Specialized Equipment and Materiel," contains a listing of associated security equipment.

- **Working and Living Areas. Buildings housing personnel and sensitive equipment should be out of grenade-throwing range from exterior fences.** Shelters with reinforced and sandbagged roofs should be near all working and living areas, to serve both as shelters and fighting positions.

- **Internal and External Territories.** Defenders must retain or deny terrain, facilities, and activities and preserve forces essential to base functions while minimizing the impact of security efforts on the local population.

- **Medical Facilities. Medical facilities should be well-marked** if the tactical commander so directs and placed away from possible lucrative targets. They must be able to augment security forces, have backup energy sources, and rely on additional personnel for security if needed.

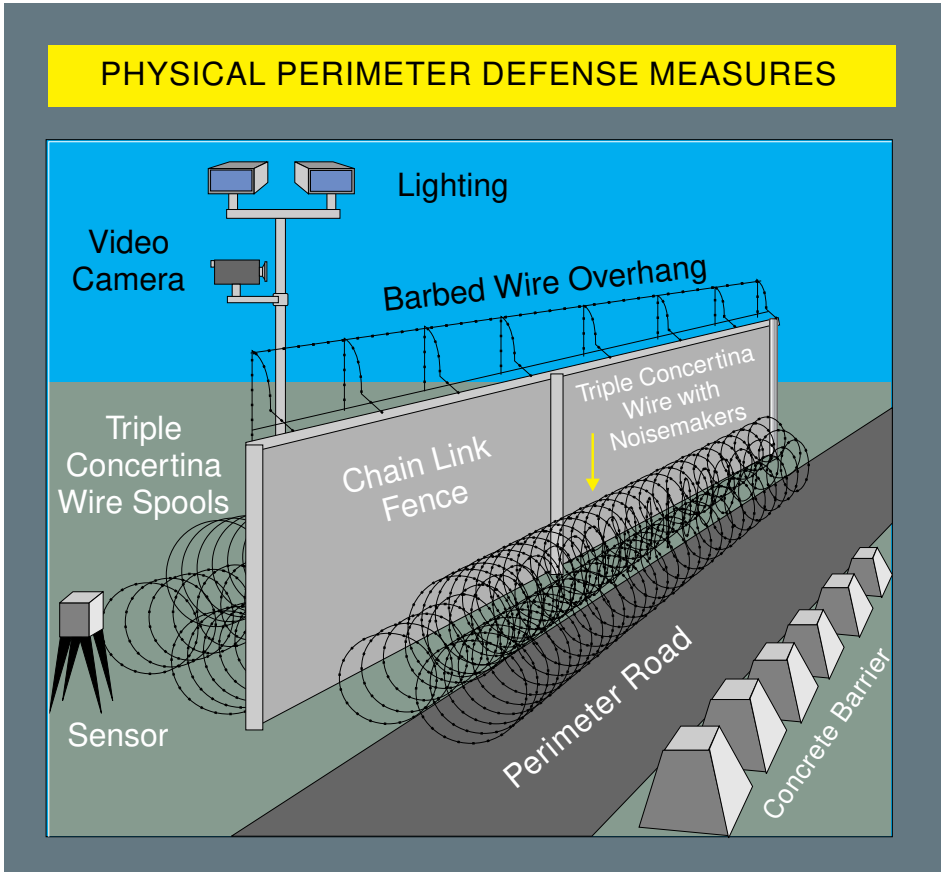


Figure IV-7. Physical Perimeter Defense Measures

p. **OPSEC Measures and Deception. OPSEC measures and deception actions should include visual, sonic, olfactory, and electronic measures.** The measures should be mutually supporting and credible. Planned patterns of physical security, reaction force operations, and other such matters should be systematically avoided.

6. Evacuation

In extreme situations, **it may be necessary to evacuate a base or part of a base, or to move essential base activities elsewhere in the JRA to perform their functions with less enemy interference**. Plans should include the identification of bases most at risk, the advantages and disadvantages of evacuation, and the conduct of evacuation operations.

CHAPTER V
HOST-NATION SUPPORT

"When two work side-by-side, one or the other spots the opening first if a kill's at hand. When one looks out for himself, alert but alone, his reach is shorter — his sly moves miss the mark."

King Nestor of Pylos
in Homer's The Iliad, x, c. 800 BC

1. General

HNS is based on bilateral diplomatic agreements that commit the HN to provide specific support under prescribed conditions. **In the majority of cases, US bases are located in friendly HNs.** Once a base is established in an HN, close cooperation with the HN and special consideration for its people, culture, and territory are vital in attaining US goals.

2. Planning for HNS of Base Defense

HNS enhances the abilities of US forces to perform their missions. **HNS can reduce requirements for US personnel, materiel and services**, allowing more flexibility in assigning forces. HNS is essential when political agreements limit the numbers of US personnel on bases. US forces should expect HNS when the HN has total sovereignty and is acting in concert with US forces to achieve strategic and operational objectives. **Factors to consider when planning HNS include those shown in Figure V-1.**

3. Base Defense Coordination

When the forces of the United States, HN, and third country allies or coalition partners occupy bases together, **special consideration must be given to the synchronization of C2 and the defense capabilities from every available source**. Commanders should address the considerations set forth in Chapter IV, "Base Defense Operations," and Appendix

Base defense plans must integrate special procedures when a host-nation labor pool is required.

PLANNING FOR HOST-NATION SUPPORT IN BASE DEFENSE

Capability, willingness, and reliability of the host nation to provide and sustain resources

Economies in US forces, equipment, and facilities made possible by using host-nation support

Effects on security, including operational security. US and host-nation counterintelligence and security agencies must develop a system to screen the backgrounds and loyalties of host-nation personnel employed on the base. There must be a detailed agreement on levels of security cooperation

Capability of US forces to coordinate host-nation support and integrate host-nation resources into base mission performance and defense

Finance support requirements for host-nation support. Finance representatives should participate in planning host-nation support. Finance elements will be required to provide contractor payments, commercial vendor services, and perform other finance tasks related to host-nation support

Figure V-1. Planning for Host-Nation Support in Base Defense

F, "Security," from a multinational perspective. Base defense plans must integrate the special capabilities and procedures for maneuver, fire support, C2, intelligence, air and missile defense, mobility and survivability, and combat service support of the units and activities of each nation represented. Plans should provide for intense multinational training programs.

4. Facilities and Systems

HN government agencies build, operate, and maintain facilities and systems such as utilities and telephone networks, and provide their services in support of US forces. Police, fire fighters, and border patrols may be available as well. US forces also may use HN facilities for hospitals, headquarters, billets, warehouses, and maintenance shops. **However, plans for HNS must consider how to use HN resources that are available in relative abundance without imposing a burden on resources the HN needs for its own development.**

5. Supplies, Services, and Equipment

a. **Bases may acquire supplies and services** such as laundry, bath, bakery, trash collection, or transportation from US, HN, or third country contractors. While in the theater, such contractors may use HN or third country personnel.

b. **Bases may need local support personnel**, such as laborers, stevedores, truck drivers, supply handlers, equipment operators, mechanics, linguists, medical aides, computer operators, and managers. Many will be available from the HN labor pool. When available, HN military or paramilitary units may support US forces by performing functions such as traffic control, convoy escort, base security, and cargo and troop transport.

c. **HNS may be provided for special functions**, such as rail operations assistance, convoy scheduling, air traffic control, and harbor pilot services. Local purchase or procurement of supplies and services, when permitted by HN agreements, may reduce the theater or joint operations area logistic requirements.

6. Command and Control

US and HN commanders retain command of their respective units, with US forces being granted support authority in order to work in fullest cooperation with HN personnel. **Base commanders should determine the type and degree of HNS which will be provided during periods of increased tension and/or conflict**. Based on the assessment of continued HNS, base commanders should develop contingency plans for potential shortfalls.

a. The degree of C2 that US forces exercise over HNS depends on the type of HNS involved, the location, tactical situation, political environment, and HNS agreements.

b. When possible, the United States coordinates its control of HN resources through local officials. CA personnel provide an interface with HN authorities.

c. The HN may provide all security to US bases or may share the responsibility for base security with US forces. Both situations require close coordination, common communications, and a detailed base defense plan.

7. NBC Defense

When required, **HN and third country military, paramilitary, and civilians providing support are equipped and trained to operate in an NBC environment**. Training and equipping are normally national responsibilities. See Appendix B, "Nuclear, Biological, and Chemical Defense."

8. Training

US personnel at all levels should receive training in dealing with HN personnel, both on and off duty. Training in the use of HN communications (telephone) systems may be appropriate. Orientation should include HN government regulations, business practices, social customs, military procedures, religious customs, and language familiarity. Frequent training in security awareness, base defense procedures, and safety should be provided to those HN units charged with support of the defense effort.

9. Intelligence

Specific provisions for multinational intelligence operations and the sharing of intelligence gained from national systems are usually arranged at the highest levels. **Base commanders must ensure that their intelligence elements link with the JFC and other joint force intelligence staffs.** HN agencies are normally excellent HUMINT and CI sources. Therefore, effective CI links should be maintained with local HN police, military, and paramilitary agencies for timely information concerning direct threats to the base.

10. Civil Affairs

Civil affairs is a responsibility of command. Base commanders can expect to conduct civil-military operations, which include establishing and maintaining military-to-civilian relations with the host nation. **Trained civil affairs personnel can provide the commander an economy of force capability to achieve assigned objectives** through direct interface with host-nation officials, agencies, and population. Refer to Joint Pub 3-57, "Doctrine for Joint Civil

Affairs," for additional guidance. PSYOP capabilities can also contribute to CA. See Joint Pub 3-53, "Doctrine for Joint Psychological Operations," for information on PSYOP in support of CA.

11. Psychological Operations

Base commanders should conduct dynamic and continuous psychological operations to promote host-nation employee loyalty to the base, promote acceptance and support for base personnel among the surrounding population, and enhance the collection of indicators and warning intelligence. **PSYOP has the capability of producing products that provide guidance to the population within the rear area concerning safety measures associated with joint rear area operations.** Posters, radio messages, and leaflets may be used to inform the local population of danger areas. PSYOP provides the rear area commander a direct link in communicating with any target groups that may affect rear area operations. Trained PSYOP personnel understand the political, economical, cultural, and social ideals of their target audience, and can therefore assist the commander in accomplishing assigned objectives. Refer to Joint Pub 3-53, "Doctrine for Joint Psychological Operations," for additional guidance.

APPENDIX A
MARITIME-LAND INTERFACE

1. Joint Base on a Shoreline

The establishment of a base on a shoreline in the JRA presents special advantages and challenges to those responsible for the functions inherent in the base's mission and for its defense. The advantages include the availability of the assets of more than one Service component for use by commanders in fulfilling their responsibilities. The special challenges may include the fact that facilities like ports and harbors are usually located in heavily populated areas. Command arrangements may be complicated by diverse purposes when multiple Service components use the same facilities. For example, the following installations may be in close geographical proximity:

a. Army common-user water terminal;

b. Support base for a MAGTF;

c. Naval base supporting and sustaining fleet operations and/or naval coastal warfare operations, naval advanced logistic support site (ALSS), and naval forward logistic site (FLS); and

d. Air Force base operating an aerial port of debarkation.

2. Command and Control

a. The JFC designates the base commander, usually from the Service component with the dominant force on the installation.

b. The JFC must designate the chain of command for security and defense, which may differ from the mission chain of command. In the case of multi-Service operations, each Service component facility may be designated a separate base as part of a base cluster commanded by the designated predominant Service commander. The base or base cluster may be directly subordinate to the joint headquarters, to a component commander, or to an area or functional commander. In the case of a large joint operation, the Army Material Command may have extensive ongoing contractor support operations (to open the port and remain throughout the operation as required). Command relationships must account for their presence and make allowance for any special protective measures. Examples of area or functional commanders are:

- Marine force service support group commander;
- Army transportation command commander, TAACOM commander, and ASG commander;
- Naval coastal warfare commander, ALSS commander, and FLS commander;
- Air Force component commander; and
- Joint special operations component commander.

3. Defense Planning

a. **Potential Threats**

- **Land-Based Attacks.** Land threats to the base include all levels of threat discussed in Chapter I, "Joint Rear Area Concepts." Procedures for defense of land approaches are discussed in Chapter IV, "Base Defense Operations."
- **Air and Missile Attacks.** Appendix C, "Air and Missile Defense," discusses the defense of the base from air and missile attacks.

- **Waterborne Attacks.** Friendly naval forces are the primary defense against waterborne threats and should achieve naval superiority in the waters adjacent to the base. However, even if overall superiority is achieved, small enemy units may seek to interfere with base operations from seaward approaches.

  •• **Amphibious Raids.** The enemy may attempt amphibious raids using watercraft and/or aircraft. Likely beaches, LZs, and insertion areas should be outposted, obstacles should be placed, and the mobile reserve employed to counter such raids.

  •• **Sea Mining.** Enemy mining of the seaward approaches to the base can be conducted from surface vessels, by air, or clandestinely by submarines. Detection of such activity should be a priority effort for surveillance systems, patrol boats, and aircraft guarding the seaward approaches to the base.

  •• **Maritime Special Operations Forces.** Determined, specially trained, organized, and equipped individuals or units can infiltrate ports, harbors, and bases near shore by swimming, scuba diving, high-speed surface craft, indigenous small boats, or miniature submersibles. They can damage vessels, port facilities, and base resources. Security forces, both seaward and ashore, and their supporting surveillance systems must be prepared to locate and counter such threats.

b. **Approaches to the Base.** Appropriate security and surveillance forces, backed up by capable mobile reserve forces, must be designated to cover every possible avenue of approach. These approaches include:

- Beaches;
- Concealed water approaches (fjords, bayous);
- Rivers;
- DZs and LZs;
- Land approaches;
- Urban terrain and infrastructure (including underground water and sewage systems); and
- Piers, docks, and waterfront facilities.

c. **Defense Forces**

- **Ground Defense Forces.** Normally, the units operating the base facilities are the most common source of personnel and equipment to form a ground defense force. For especially critical facilities, dedicated defense forces such as Marine Corps security forces, Air Force security police, Army military police, or Marine Corps military police units may form the core of the ground defense effort.
- **Air and Missile Defense.** See Appendix C, "Air and Missile Defense."
- **Navy and Coast Guard Organizations.** The naval coastal warfare commander (NCWC) may form a port security and harbor defense group (PSHDGRU) to support defense efforts. The harbor defense commander (HDC) sets the boundaries for harbor defense for the PSHDGRU. Defense of the harbor is the responsibility of the HDC, and inland defense is the responsibility of the appropriate area or component commander designated by the JFC. Close coordination on mission priorities must be accomplished for naval coastal warfare units between the NCWC and base commander to avoid conflicts. On

a larger scale, under the direction of the NCWC, the PSHDGRU may have OPCON of forces providing port security and harbor defense in more than one port and/or harbor. This may be particularly true along a coastline that has multiple ports in geographic proximity to each other. In this situation, the multiple ports may be designated a base cluster. The PSHDGRU will, through the NCWC, coordinate security operations with the appropriate area or functional commander. The PSHDGRU may possess some or all of the following capabilities.

•• **Mobile Inshore Undersea Warfare Unit.** A mobile surveillance and detection unit that possesses surface radar, subsurface sonobuoy, swimmer detection and neutralization, and naval communications capabilities.

•• **Naval Explosive Ordnance Disposal (EOD) Detachment.** This detachment provides ordnance handling and evaluation, special weapons and/or ammunition support, and mine detection and neutralization capabilities. This detachment also identifies mine and/or ordnance beaching areas for the port or harbor.

•• **Port Security Unit (PSU).** This unit is provided by the US Coast Guard and is integrated into the Navy component in wartime or as allowed by law. The mission of a PSU is to conduct outside the continental US port security and/or harbor rear area operations in support of requesting combatant commanders. Port security elements include patrolling harbors and anchorages, maritime interdiction, surveillance, and the enforcement of exclusionary zones.

•• **Mine Countermeasures (MCM) Elements.** These elements detect and destroy enemy mines in harbors, approaches, and sea lanes, using mine countermeasure aircraft and vessels. Because of the small number of MCM forces, control of these assets is normally determined by the Navy component commander.

•• **Mobile Diving and Salvage Unit (MDSU).** The MDSU has the missions of underwater hull search and repair, channel clearance, vessel salvage, and pier and piling inspection and repair. The PSHDGRU commander can request this unit's support of base defense efforts from the NCWC when required.

•• **Naval Special Boat Unit (SBU) Detachments.** SBU detachments are organized to conduct or support joint special operations and coastal patrol and interdiction with coastal and riverine craft. SBU detachments consist of various high-speed small craft up to the 175-foot ships of the Cyclone (PC-1) class. Most craft can mount crew-served weapons. When available and pending other priorities, the detachments can be requested to support base defense.

4. Planning Considerations

The following factors should be considered when planning the defense of a base on a shoreline.

a. Type and nature of the threat.

b. Protection for sea approach chokepoints.

c. Tides and currents.

d. Water clarity and depth.

e. Pier clearance.

f. Lighting.

g. Use of patrol boats.

h. Communications.

i. Rail and highway entrances security.

j. Air and missile defense measures.

k. Security for individual vessels.

l. Area damage control.

APPENDIX B
NUCLEAR, BIOLOGICAL, CHEMICAL DEFENSE

1. General

Every base commander integrates NBC defense measures designed to detect, defeat, and minimize the effects of NBC attacks. Units occupying bases in the JRA must plan and train to perform their missions in an NBC environment if necessary. Joint Pub 3-11, "Joint Doctrine for Nuclear, Biological, and Chemical (NBC) Defense" provides guidance for joint NBC defense.

2. Fundamentals

There are three fundamentals of NBC defense: contamination avoidance, protection, and decontamination.

a. **Contamination Avoidance.** This fundamental is the most difficult to implement on bases in the JRA because of the immobility of bases. However, some effects may be avoided or minimized by taking the following measures.

- Take passive measures to prevent the enemy from selecting the base as a target, such as using camouflage, concealment, deception, and dispersion. Smoke may be used to enhance concealment measures.

- Detect and identify hazards. Monitor for contamination, reconnoiter, and survey specific areas to determine contamination status.

- Use the NBC warning and reporting system. When a hazard is detected, pass the alarm locally and then warn others by using the standard warning and reporting systems. If detailed surveys are conducted later to determine the actual extent of contamination, the results of these surveys also should be disseminated using the standard reporting formats.

- Limit contamination spread. Cover equipment vital to mission accomplishment before attack to prevent unnecessary contamination; use only mission-essential equipment when contamination is present; and restrict personnel movement in the contaminated area.

- Move from the contaminated area when the mission permits. However, avoid spreading or carrying the contamination during movement.

- If required, evacuate biological and unknown chemical agent samples through intelligence channels to a laboratory for identification.

b. **Protection.** Protection is required when contamination cannot be avoided. Doctrinal manuals discuss NBC protection in detail. Protection is divided into three broad areas: force protection, individual protection, and collective protection.

- Force protection involves actions taken by a commander to reduce force vulnerability to NBC attack. On small bases, this will require that the unit conduct a procedure called mission-oriented protective posture analysis. However, several other decisions concerning alarm placement, automatic masking, and other types of decisions will be required as part of the analysis. Forces on large bases or base clusters will conduct a process called vulnerability assessment and risk reduction. The vulnerability assessment is an estimate of the probable impact on the force of an

enemy NBC attack. It occurs both before and after initiation of NBC warfare.

- Individual protection involves those measures each person must take to survive and continue the mission. It includes the specific actions required for maximum protection against NBC hazards with minimum loss of efficiency. Members of base units must be equipped with individual protective clothing and equipment. All must be proficient in protective measures to take before, during, and after an NBC attack. Mission-essential US and HN civilians working on the base must be trained and equipped to ensure their survival. Crews of naval and merchant vessels in ports also must be prepared for NBC attacks.

- Collective protection should be an integral part of NBC countermeasures. Collective protection provides selected contamination-free working environments and allows personnel relief from continuous wear of NBC protective clothing. Collective protection is required in accordance with individual Service directives. Examples of areas normally requiring collective protection are listed below.

  •• Command posts and communications centers.

  •• Fire direction centers.

  •• Missile control complexes.

  •• Combat vehicles.

  •• First-aid stations and hospitals.

  •• Rest and relief stations.

  •• Fixed-site logistic facilities.

c. **Decontamination.** Decontamination is the reduction of the contamination hazard by removal or neutralization of hazardous levels of NBC contamination on personnel and materiel. The primary purposes of decontamination are to stop erosion of combat power and reduce casualties that may result from inadvertent exposure or failure of protection. Initial decontamination may be performed by base personnel. Detailed decontamination may require requesting assistance from chemical units assigned to support area commanders in accordance with JRAC priorities. Service manuals discuss decontamination in detail. Decontamination sites should be established in the base area and decontamination supplies should be prestaged before an anticipated NBC attack. Some planning considerations follow.

- Identify hasty and deliberate decontamination sites.

- Designate decontamination teams and ensure that they have the necessary equipment and command and control assets.

- Plan for treatment of contaminated casualties.

- Plan for the marking and reporting of contaminated areas and terrain decontamination.

- Plan for employment of detection alarms.

- Conduct necessary NBC training.

- Plan for disposal of the waste products of decontamination operations.

3. Other NBC Considerations

a. **Obscurants.** Employ obscurants to improve survivability during windows of

increased vulnerability, such as imminent air attacks, command post displacements, or critical operations like fast refueling or main supply route repair. Employ deceiving smoke in conjunction with electronic and physical deception measures to mislead the enemy. Use smoke to disrupt enemy surveillance and target acquisition means.

b. **Flame Weapons.** Incorporate flame weapons, if available, into barrier plans. Use flame weapons to destroy and demoralize enemy forces and illuminate the battlespace.

Intentionally Blank

APPENDIX C
AIR AND MISSILE DEFENSE

1. Active Air and Missile Defense

Some bases in the JRA have limited capability to engage and destroy incoming enemy aircraft and missiles; therefore, commanders must be aware of the assets that they do possess and use them to maximum effect.

a. **Integration With Other Air Defense Assets of the Joint Force.** Some bases by their nature possess special capabilities for active air and missile defense. Bases with air defense missile units and counterair and/or antiair warfare aircraft play important roles in the overall theater and/or joint operations area air defense. These units are subject to the weapon control procedures of the AADC and airspace control authority (ACA). For details concerning the integration of air defense efforts in the JRA see Joint Pub 3-10, "Doctrine for Joint Rear Area Operations," and Joint Pub 3-52, "Doctrine for Joint Airspace Control in the Combat Zone."

b. **Air and Missile Defense Weapons Organic to Base Units.** More pertinent to the close-in defense of the base are the weapons possessed by base units. Many ground units are equipped with small arms (M-2 and M-60 machine guns, squad automatic weapons, and M-16 rifles). Air defense systems like Patriot, Hawk, and Stinger may be assigned to bases in JRA for point defense of critical installations. Navy antiair warfare assets on ships in harbors or offshore, such as standard missiles and close-in weapon systems, may be available to augment the base air and missile defense posture. The base commander must ensure that all base air and missile defense assets are coordinated with appropriate airspace control authorities, often by the establishment of base defense zones (BDZs) and short-range air defense engagement zones in coordination with the AADC and ACA. The training of weapon crews in ROE is essential to prevent fratricide.

2. Passive Air and Missile Defense Measures

The objective of passive air and missile defense is to degrade the enemy's ability to target US and HN or multinational forces and facilities, reduce vulnerability to attack, and provide for reconstitution and recovery of forces.

a. **Air Defense Warning.** Air defense warning is a trigger event for passive defense measures by non-air-defense assets. Air defense warnings are normally issued by the AADC and are categorized as red (hostile attack imminent), yellow (probable), or white (improbable). Air defense assets will initiate engagements sequences to counter aircraft and missiles threats in accordance with established air defense control measures, ROE and specific directives issued by the AADC.

b. **Reducing Targeting Effectiveness**

- **Operations Security.** Such OPSEC measures as transmission security, signature reduction, smoke, dummies, and pattern painting deny enemy sensor and reconnaissance assets accurate and timely acquisition and identification of friendly targets. Signature reduction measures include camouflage, commonality of vehicle appearance, emission control programs for infrared and electromagnetic emissions, and cover and concealment. Local unit security is

an important element in denying accurate targeting data to enemy special operations forces or other enemy agents.

- **Military Deception.** Military deception shapes the enemy's intelligence by conveying or denying data to their intelligence system. The intent is to influence their actions to our advantage or to guard the secrecy of our actions. Deception normally will be employed as OPSEC measures.

- **Mobility.** Mobility, especially when combined with concealment, deception, and dispersal, can create uncertainty for the enemy as to whether they have found a key asset or a decoy. Mobility also creates uncertainty as to whether that asset will still be there when the enemy attacks it.

c. **Reducing Vulnerability**

- **Hardening.** Hardening reduces the effect of attack on aircraft, base support equipment and facilities, nuclear delivery systems and storage areas, C2 nodes, and other facilities. Hardening measures should commence before hostilities if possible. Field expedients should be replaced by permanent fortifications as time and resources permit.

- **Dispersal.** Dispersal reduces target vulnerability by increasing the distance between friendly assets. However, dispersal also will increase the difficulty of defending from a ground attack and frequently will reduce the efficiency of base operations.

- **Training Civilian Authorities.** Local authorities should be trained to organize and instruct their populations to protect themselves from air and missile attack. Effective training of this nature will reduce the physical and emotional impact of such attacks.

d. **Reconstitution and Recovery.** Following an attack, units must be restored to a desired level of combat effectiveness commensurate with mission requirements and available resources. Reconstitution may include reestablishing or reinforcing C2, reallocating or replacing personnel, supplies, and equipment, conducting essential training, reestablishing unit cohesion, and repairing damage.

APPENDIX D
BASE DEFENSE OPERATIONS CENTER

1. The Base Defense Operations Center

a. There is no standard organization for a BDOC. Just as the size, type, and classification of bases vary, so does the organization of the BDOC.

b. The base commander must form the BDOC from available base assets. There are several options regarding the location and status of the BDOC.

- A base mission operations center also performs BDOC functions. This option is possible when the functions of the base can be interrupted in order to conduct defensive operations. The base staff becomes the base defense staff.

- BDOC is adjacent to the base mission operations center. Base defense operations are conducted while the base's primary mission continues. The defense function is separate from the mission, but proximity permits a high degree of coordination and possible sharing of physical facilities such as communications and messing.

- BDOC is separate from the base mission operations center. This option may be forced by the necessity to occupy separate facilities or may be selected to ensure that the two functions do not mutually interfere.

c. **Support**

- During low-threat periods the BDOC may be able to function with austere support. Only sufficient personnel and equipment to supervise security efforts and process long-range intelligence may be necessary. Most base personnel can then concentrate their efforts on the base's primary mission, although all personnel should rehearse base defense procedures.

- As the threat to the base is perceived to increase, more base units and personnel are diverted from mission tasks to their defense responsibilities. As a result, the BDOC evolves, as planned, into an operations center capable of controlling a full-scale defense of the base.

2. Notional BDOC

When fully augmented for controlling the defense of the base against full-scale attacks, the BDOC should be structured with the following functional elements. Numbers of personnel in each element depend on base size and the requirements for 24 hour operations. Some functions may be performed by other C2 activities on the base. Paragraph 3 discusses base defense facilities on an Air Force installation.

a. **Operations Element**

- BDOC chief (Commander, Base Defense Force).

- Operations personnel.

- NBC personnel.

- Engineer representative.

- MP or SP representative.

- Legal personnel.

b. **Intelligence Element**

- Intelligence personnel.

- CI personnel.

c. **Fire Support Element and Fire Support Coordination Center.** If attached, Air Force, Navy, Marine air, Army air defense, naval gunfire, and special operations liaison personnel will join the FSE/FSCC to form a fire support cell. Normally, a BDOC will not be provided an FSE/FSCC, in which case the function will be performed by the BDOC operations element.

d. **ADC Element**

e. **Civil-Military Operations Element**

f. **Communications Element**

g. **Liaison Teams**

- RAOC/RTOC liaison officer (LNO).

- HN representative.

- Tactical combat force LNO.

- Intelligence and CI liaison personnel.

h. **Medical Element**

3. Air Force Base Defense

a. The base commander, operations personnel, NBC personnel, base civil engineering representatives and CI personnel from the Air Force Office of Special Investigations (AFOSI) are located at the Survival Recovery Center.

b. Damage control and EOD personnel are located at the Damage Control Center.

c. The BDOC on Air Force installations consists of security personnel, fire support representatives (including naval gunfire support if available), and HN representatives.

d. The SP chief works for the senior installation commander and acts as the commander's executive agent for ground defense (ground defense force commander) operating the BDOC. Personnel from AFOSI and wing intelligence functions or sections provide their information to the BDOC intelligence section.

4. Level I Threat Considerations

In the Level I threat environment, the BDOC may take the form of a regional coordination center, including civilian advisers. BDOC can coordinate US and HN military and civilian activities and coordinate the politico-military battle.

APPENDIX E
SAMPLE BASE DEFENSE PLAN

(In Joint Operation Order [OPORD] Format)
SECURITY CLASSIFICATION

Copy No. _____
Issuing Headquarters
Place of Issue
Message Reference Number

Type and Serial Number of Operation Order.

References:

a. Maps or Charts

b. Time Zone. (Insert the time zone used throughout the order)

Task Organization. (List this information here, in paragraph 3, or in an annex if voluminous. The organization for defense should clearly specify the base units providing the forces for each defense element. Attached or transient units and the names of commanders should be included. The defense requirements of US, HN, and other civilian organizations quartered on the base also should be identified. Their capabilities to assist in the defense must be determined and integrated into the base defense plan.)

1. Situation. (Under the following headings, describe the environment in which defense of the base will be conducted, in sufficient detail for subordinate commanders to grasp the way in which their tasks support the larger mission.)

a. Enemy Forces. (Describe the threat to the base, to include the composition, disposition, location, movements, estimated strengths, and identification and capabilities of hostile forces, including terrorist organizations.)

b. Friendly Forces. (List information on friendly forces not covered by this operation order, to include the mission of the next higher headquarters and adjacent bases as well as units not under base command whose actions will affect or assist the defense of the base. These units may include MP or Air Force SP response forces, fire support, naval coastal warfare forces, special operations forces, engineers, NBC decontamination or smoke units, EOD, HN military or police organizations, and public and private civilian organizations of both the United States and HN.)

c. Attachments or Detachments. (When not listed in the Task Organization, list elements attached to or detached from base units and the effective times.)

2. Mission. (Give a clear, concise statement of the commander's defense mission.)

3. Concept of the Operation. (Under the following headings, describe the commander's envisioned concept of the operation.)

a. Commander's Intent. (The commander discusses how the development of the defense is envisioned and establishes overall command priorities. This subparagraph should provide subordinates sufficient guidance to act upon if contact is lost or disrupted.)

b. Concept of Operation. (Briefly describe how the commander believes the overall operation should progress. Define the areas, buildings, and other facilities considered critical, and establish priorities for their protection.)

(1) Phasing. (Set forth, if necessary, the phases of the operation as they are anticipated by the commander.)

(2) Maneuver. (Describe the organization of the ground defense forces, the assignment of elements to the security area to primary, alternate, and supplementary defensive positions, and to the base rear area. Describe the purpose of counterattacks and set work priorities.)

(3) Fires. (State plans for employing supporting fires, such as mortars and other indirect fire assets, smoke, and aviation support.)

c. Tasks for Subordinate Elements. (If not previously described, this and succeeding subparagraphs should set forth the specific tasks for each subordinate defense element listed in the Task Organization.)

d. Reserve. (The next-to-last subparagraph of paragraph 3 contains instructions to the base's mobile reserve.)

e. Coordinating Instructions. (Always the last subparagraph of paragraph 3. Contains those instructions applicable to two or more elements or to the command as a whole.)

(1) Control Measures. (Define and establish restrictions on access to and movement into critical areas. These restrictions can be categorized as personnel, materiel, and vehicles. Security measures also may be outlined here.)

(a) Personnel Access. (Establish control pertinent to each area or structure.)

1. Authority. (Give authority for access.)

2. Criteria. (Give access criteria for unit contractor personnel and local police and armed forces.)

3. Identification and Control

a. (Describe the system to be used in each area. If a badge system is used, give a complete description to disseminate requirements for identification and control of personnel who conduct business on the base.)

b. (Describe how the system applies to unit personnel, visitors to restricted or administrative areas, vendors, contractor personnel, and maintenance and support personnel.)

(b) Materiel Control Procedures

1. Incoming

a. (List requirements for admission of materiel and supplies.)

b. (List special controls on delivery of supplies to restricted areas.)

2. Outgoing

a. (List required documentation.)

b. (List special controls on delivery of supplies from restricted areas.)

c. (List classified shipments.)

(c) Vehicle Control

1. (State policy on registration of vehicles.)

2. (State policy on search of vehicles.)

3. (State policy on parking.)

4. (State policy on abandoned vehicles.)

5. (List controls for entering restricted areas.)

(d) Train Control

1. (State policy on search of railcars.)

2. (State policy on securing railcars.)

3. (State policy on entry and exit of trains.)

(2) Security Aids. (Indicate the manner in which the following security aids will be implemented on the base.)

(a) Protective Barriers

1. Definition.

2. Clear zones.

a. Criteria.

b. Maintenance.

3. Signs.

a. Types.

b. Posting.

4. Gates.

a. Hours of operation.

b. Security requirements.

c. Lock security.

d. Protective lighting system. (Use and control, inspection, direction, actions during power failures, emergency lighting.)

(b) Intrusion Detection System

1. Types and locations.

2. Security classifications.

3. Maintenance.

4. Operation.

5. Probability of Detection.

a. Limitations.

b. Compensating measures.

c. Redundant capabilities.

(c) Communications

1. Types.

a. Primary

b. Alternate

2. Operation.

3. Maintenance.

4. Authentication.

(3) Interior Guard Procedures. (Include general instructions that apply to all interior guard personnel, fixed and mobile. Attach detailed instructions such as special orders and standing operating orders [SOPs] as annexes. Ensure that procedures include randomness.)

(a) Composition and organization. (NOTE: In military operations other than war environment, the interior guard may be a contracted civilian security force.)

(b) Tour of duty.

(c) Essential posts and routes.

(d) Weapons and equipment.

(e) Training.

(f) Military working dogs.

(g) Method of challenge.

(h) Alert force.

1. Composition.

2. Mission.

3. Weapons and equipment.

4. Location.

5. Deployment concept.

(4) Rules of Engagement. (Coordinate and control the use of force to prevent fratricide.)

(5) Contingency Plans. (Indicate actions in response to various emergency situations. List as annexes any detailed plans, such as combatting terrorism, responding to bomb threats and hostage situations, dealing with disasters, and firefighting.)

(a) Individual actions.

(b) Alert force actions.

(6) Security Alert Status

(7) Air Surveillance

(8) Noncombatant Evacuation Operation Plans

(9) Coordination With HN or Adjacent Base Plans

(10) Measures for Coordination With Response Force and Tactical Combat Forces

(11) Procedures for Update of This OPORD. (If the OPORD is not effective upon receipt, indicate when it will become effective.)

4. Administration and Logistics. (This paragraph sets forth the manner of logistic support for base defense. State the administrative and logistic arrangements applicable to the operation. If the arrangements are lengthy, include them in an annex or a separate Administrative and Logistics Order. Include enough information in the body of the order to describe the support concept.)

a. Concept of Combat Service Support. (Include a brief summary of the base defense concept from the combat service support point of view.)

b. Materiel and Services. (List supply, maintenance, transportation, construction, and allocation of labor.)

c. Medical Services. (List plans and policies for treatment, hospitalization, and evacuation of both military and civilian personnel.)

d. Damage Control. (List plans for firefighting, clearing debris, and emergency construction.)

e. Personnel. (List procedures for strength reporting, replacements, and other procedures pertinent to base defense, including handling civilians and prisoners of war.)

f. Civil Affairs. (Describe control of civil populations, refugees, and related matters.)

5. Command and Signal

a. Communications. (Give information about pertinent communications nets, operating frequencies, codes and code words, recognition and identification procedures, and electronic emission constraints. Reference may be made to an annex or to a SOI.)

b. Command

(1) Joint and multinational relationships. (Command relationships must be spelled out clearly, to include command succession. Shifts in relationships as the defense progresses, as when a response force is committed, must be specified. These relationships may be presented in chart form as an annex.)

(2) Command posts and alternate command posts. (List locations of the BDOC, BCOC, and their alternate sites, along with the times of their activation and deactivation.)

6. Acknowledgment Instructions

Annexes:

A. Task Organization
B. Intelligence
C. Operations
D. Logistics
E. Personnel
F. Public Affairs
G. Civil Affairs
H. Engineer Support
J. Command Relationships
K. Command, Control, and Communications
L. Force Protection
M. Host-Nation Support
N. NBC Defense

Distribution:

Authentication:

Intentionally Blank

APPENDIX F
SECURITY

Security is the primary concern under threat Level I, especially if the base is located in an urban area.

SECTION A
TACTICAL SECURITY

1. Patrols

Patrolling is necessary outside the physical base but within the AO to provide additional base security. Patrolling urban areas involves different risks and considerations than patrolling open or cleared uninhabited areas. Patrolling may require the use of military working dogs. A patrol is tasked to collect information, confirm or deny accuracy of previously gained information, provide security, and harass, destroy, or capture the enemy. The two categories of patrol are reconnaissance and combat. Patrols can be conducted dismounted or mounted.

a. **Dismounted Patrols.** A patrol may be a fire team, squad, platoon, or company. Patrol members must be able to interact with local inhabitants but still should be ready to conduct combat operations. Multiple units maintain mutual support for each other as they move and operate.

b. **Mounted Patrols.** Mounted patrols are especially useful in an economy of force mission where the unit has a large sector to cover and few personnel to patrol. Mounted patrols can be used to cover gaps between units in the defense, provide flank security and coordination, patrol forward of the base perimeter to provide early warning, and assist in reconnaissance when a large sector must be covered in a relatively short time.

- **Organization and Preparation.** The leaders of the patrol must analyze the mission, determine what elements are needed, and decide how to accomplish the mission.

  •• The patrol leader must consider route selection, linkup procedures, resupply, signal plan, departure from and reentry to base defense positions, and other friendly units in the area. Recognition signals must be firmly established to provide early and immediate identification by friendly forces.

  •• A map, ground, or aerial reconnaissance by the leader will help balance the size of the area, the time constraints of the mission, and the patrol's security requirements.

- **Fundamentals of Movement.** Inherent in all mounted patrol operations is the command and control of movement. Communications and maintenance are vital because they support movement.

  •• Competent navigation and aggressive leadership are vital ingredients to movement. Movement techniques must be understood at all levels of command. An important requirement for a mounted patrol is for the patrol to see the enemy first. The global positioning system should be used, if available.

  •• Once the enemy is sighted or encountered, the patrol moves to accomplish its task.

  •• While moving, a patrol must maximize cover and concealment using the terrain. The leader must weigh the degree of security allowable against the required speed of execution to minimize the risk to the patrol.

•• A mounted patrol should never enter a major cross compartment without first establishing security and visually inspecting the area. Mounted patrols should make maximum use of dominating overwatch positions that offer good observation and fields of fire. Elements occupying overwatch positions must do the following: (1) Visually check the security of the position and be prepared to dismount to secure the area; (2) Occupy covered or concealed positions; (3) Cover the areas for observation and fire assigned by the element leader; (4) Orient weapons on likely or suspected enemy positions; and (5) Search for and be alert for enemy activity.

- A mounted patrol must:

  •• Be alert for unusual people, vehicles, or incidents close to the beginning and end of the patrol route;

  •• Avoid the same daily routes and times;

  •• Avoid isolated routes and stops;

  •• Lock vehicle doors when appropriate;

  •• Stop short of unusual objects or incidents and investigate as required by mission;

  •• Detour around suspicious obstacles or stop and investigate as mission requires;

  •• Continually check to the rear;

  •• Be aware of vehicles' capabilities; and

  •• Use and practice movement techniques such as traveling overwatch and bounding overwatch.

2. Roadblocks and Checkpoints

A roadblock is used to limit the movement of vehicles along a route or to close access to certain areas or roads. Checkpoints are manned locations used to control movement. A roadblock is used with a checkpoint to channel vehicles and personnel to the search area. Roadblocks may be set up on a temporary or surprise basis or may be semipermanent in nature.

a. Roadblocks are used to:

- Maintain a continuous check on road movement, apprehend suspects, and prevent smuggling of controlled items;

- Prevent infiltration of unauthorized civilians into or through a controlled area;

- Check vehicles for explosive devices; and

- Ensure proper use of routes by both civilian and military vehicles.

b. Because roadblocks cause considerable inconvenience and even fear, ensure that the civilian population understands that the roadblocks are preventive and not punitive measures.

c. Roadblocks and checkpoints may be either deliberate or hasty. The deliberate roadblock or checkpoint is a relatively fixed position on the base, in a town, or in the open country, often on a main road. It acts as a useful deterrent to unlawful movement. The hasty roadblock or checkpoint is highly mobile and is quickly positioned on the base, in a town, or in the open country. Its actual location is designed to achieve surprise.

d. Conceal the roadblock or checkpoint, when appropriate. The location should make it difficult for a person to turn back or reverse a vehicle without being observed. Positions beyond sharp curves have the advantage that drivers do not see the checkpoint in sufficient time to avoid inspection. However, the checkpoint should be positioned so that drivers can stop safely.

e. A roadblock or checkpoint requires adequate personnel to provide security. A security force is concealed an appropriate distance from the roadblock or checkpoint to prevent the escape of any vehicle or person attempting to turn back upon sighting the checkpoint. The vehicle, driver, and passengers are searched. If possible, the area designated for searching vehicles is below ground level to deflect an explosive blast upward.

f. For a roadblock or checkpoint to be effective, special measures are required.

- **Signs.** Portable signs in the native language and in English must be available. Signs should denote the speed limit of approach, vehicle search area, vehicle parking area, male and female search areas, and dismount point.

- **Lights.** Adequate lighting is essential for the search area at night.

- **Communications.** Radio or land line communication is required among the various locations supporting the checkpoint operation. These include the security position, the search area, and the BDOC.

- **Barriers.** Obstacles across the road and around the search area should be provided. Obstacles must be strong and big enough to prevent motorists from driving through or around them.

- **Firepower.** Security personnel must have adequate firepower to withstand an attack or halt a vehicle attempting to flee or crash through the checkpoint.

- **Linguists.** Personnel familiar with the native language are essential at all roadblocks and checkpoints.

g. **Establishment of Roadblocks and Checkpoints.** Each roadblock and checkpoint is established by placing two parallel obstacles across the road. In addition to having barriers large enough to prevent someone from running over or through them, barriers should have gaps negotiable only by slowly moving vehicles.

- The separation between obstacles depends on the amount of traffic to be held in the search area. The blocked section of road can be used as the search area. If possible, there should be a place adjacent to the road where large vehicles can be searched without delaying the flow of traffic.

- Areas are required for searching suspects of both sexes and for detaining persons for further interrogation. Personnel manning a checkpoint should include a member of the local police, a fluent interpreter, EOD personnel, and trained females for searching other females. When a vehicle is being searched, the occupants should stand clear of the vehicle and be searched concurrently. The vehicle searcher should use an assistant to watch the occupants and provide additional security. If available, explosive detectors and dogs may be used to aid the search. Politeness and consideration should be shown to the extent consistent with a thorough search, and roadblock or checkpoint personnel should be thoroughly familiar with the limits of their legal authority.

3. Urban Defense

Base forces may be employed in urban areas for security operations or for other tasks short of conventional combat; for example, protection of facilities or equipment required for base operations. Masonry structures and other urban features can be adapted to provide protection.

a. **Security Precautions.** When employed in urban areas, commanders must estimate the threat and plan for the defense. In addition, they should consider the following security precautions.

- Wire fences or barriers for additional protection.
- Screens made of canvas or corrugated iron, for use outside buildings or inside windows. Mesh or chain-link barriers placed in front of bunkers or above-ground fighting positions aid in premature detonation of rocket-propelled grenades and other similar shaped-charge explosive devices.
- Canopies of chain-link, weld mesh, or corrugated iron. These will protect roofs if they are placed at least 1 meter above the roofs. Sandbags placed directly on roofs will absorb shrapnel.
- Obstacles in the approaches will slow or stop vehicles and personnel approaching the defended area. However, the entrance gate design must allow access to those authorized, deny access to others, and provide protection to those who must have access. If possible, illuminate fences, entrance gates, and obstacles. Cover with observation and fire.
- Sentry posts for round-the-clock security. If field fortifications are required, dig fighting positions rather than build towers. Ordinarily, sentry posts are doubled during darkness or poor visibility. Sentries should report at irregular intervals within a specified time period and be posted at:
  - •• Entrances, to check entry permits;
  - •• Observation posts or rooftops, to observe all avenues of approach and dominate buildings and grounds; and
  - •• Perimeter sites.

b. **Employment of Sentries.** Sentries must be properly trained and equipped. Some security operations may require the use of military working dogs. Sentries must be briefed on the ROE and appropriate use of force. They must be able to call on the base mobile reserve for assistance. Sentries employed in urban areas must:

- Detect and deter anyone seeking to gain unauthorized access to the secured area;
- Prevent damage, arson, and looting within the secured area;
- Ensure the maintenance of essential services; and
- Be briefed on friendly forces operating in the area such as patrols, OPs and LPs, and other adjacent unit activities.

4. Convoy Defense

Convoys on large bases or between bases are arranged for control and protection using armored vehicles, military police escort, or aerial escort, if available. Road movement is always vulnerable in high-threat areas. The convoy commander should plan convoy movements and practice using hardened vehicles if support from combat units is not available. Each convoy is organized into an advance party, main body, and trail party. The convoy commander estimates the situation

and develops a plan, to include a briefing for all convoy members. The briefing should include the following.

a. Enemy situation and capabilities, terrain, and weather.

b. Composition and order of march.

c. Chain of command and location of leaders.

d. General security posture.

e. Communications and signals.

f. Objectives.

g. Routes, schedules, and other control measures.

h. Emergency actions, actions on contact, and actions at halts.

5. Searches

a. **Personnel.** Personnel searches may be required to maintain the safety and security of the command. Quick body searches or detailed body searches may be conducted, consistent with the security environment and respect for the individual being searched. Metal detection systems should be used if available.

b. **Buildings**

- When preparing to search buildings, use radios (search net and command net) and call signs for teams and specialists. Use grid references for location of teams, control points, and headquarters. In addition, consider electronic warfare constraints.

- Assume that any unoccupied house or building is booby-trapped. Position supporting fire elements (machineguns, mortars) to cover the roofs and adjacent buildings. Begin search from roof if possible. Mark cleared room windows with sheets or blankets. Arm search teams with grenades, shotguns, and light machineguns. Visually scan the exterior for suspicious signs. Set up a command post outside and detail one pair of searchers to make the initial entry. Avoid obvious entryways and, if possible, use holes in walls and roofs. Check doors and windows for booby-traps before entering. Clearly mark with white tape the routes through the building that have been cleared. Once the building is cleared of traps, the team leader will allocate teams of searchers to make detailed room searches. If possible, avoid all radio transmissions from within buildings being searched.

- Military working dogs, if available, can be used to search for arms, ammunition, explosive caches in buildings, open areas, and routes to be cleared.

- Local officials should accompany search teams. If the building is occupied, an occupant should accompany the team.

6. Ambushes

Planned ambushes are surprise attacks by fire from concealed positions on a moving or temporarily halted enemy. However, in urban areas, ambushes are often designed to apprehend wanted persons, not necessarily to kill them. Urban ambushes should be planned to avoid harm to civilians and should be coordinated with HN forces. Sites for ambushes should be carefully planned considering the latest intelligence about hostile groups or persons.

7. Responses to Attacks

When responding to an attack from an urban area, defenders must try to kill or

capture assailants while keeping the base secure. Defenders also must consider:

a. Returning fire according to ROE;

b. Submitting a contact report, including the location, numbers of casualties, and estimated opposition;

c. Dispatching sufficient force to engage the enemy;

d. Estimating the civilian situation;

e. Establishing roadblocks on likely escape routes;

f. Deploying cordon sentries, as necessary;

g. Alerting local authorities;

h. Recovering and aiding hostages; and

i. Securing the scene for collection of evidence.

8. Crowd Control

a. Crowd violence may be a spontaneous emotional eruption, or it may be a planned event. In the latter case, the purpose may be to draw attention away from something else or to draw people to a location where attack is easier. Crowd violence may involve civilian group interaction. Mob violence is highly contagious. The aim of riot control is to restore order as quickly as possible, with minimum force, and return control to civilian authorities. HN police agencies should assume principal responsibility for countering actions of indigenous personnel. US forces should come into direct conflict with indigenous personnel only in emergency situations when HN police or military personnel are not present.

b. The best way to disperse rioters is to make key arrests and simultaneously demonstrate the ability to disrupt the activities of the remaining rioters. Separation from leaders combined with the likelihood of apprehension and the denial of unrestricted actions can have a debilitating effect on mob activities. Leave an escape route open to allow rioters to disperse. The HN police force must assist. Once the crowd has dispersed and all is quiet, return troops to the assembly or base area. Try not to escalate the violence by misuse of force. The use of riot control agents must follow stated national policy and HN agreements. Close coordination with legal counsel and US diplomatic missions may be necessary.

c. PSYOP may be an effective measure in crowd control. PSYOP tactical loudspeaker units can disseminate pre-recorded messages encouraging dispersal. These units provide the commander a quick response method to communicate intent to a possibly hostile crowd.

SECTION B
UNIT SECURITY

9. Planning

a. **Mission Analysis.** To perform a mission analysis, ask the following questions.

- How can the mission be adversely affected by an attack?
- What are the security aspects of both specified and implied tasks?

b. **Threat Assessment.** Coordinate with intelligence and CI personnel to identify sources of information on insurgent and terrorist groups. Know how to access these sources quickly and routinely. Include threat assessment in intelligence estimates as a continuing process. Identify insurgent and terrorist groups operating in the deployment area. Develop a list of PIR, including:

- Methods of operation;
- Attack methodology; and
- Preattack indicators.

c. **Support Considerations.** To implement unit security, the following areas should be considered.

- **Supply.** Procure special security equipment, such as detectors, portable barriers, and intrusion detection devices. Protect storage and distribution areas.
- **Maintenance.** Maintain special equipment and provide security to maintenance units.
- **Transportation.** Provide security during movement and in staging areas and provide liaison with security agencies such as area MP organizations supporting movements.
- **Engineer.** Provide security and ADC measures and special engineer equipment.
- **Base Military or Security Police.** Check, inspect, and improve unit physical security. Provide liaison with local police and security personnel. Screen US and HN civilian employees.
- **Health Services Support.** Ensure security of medical facilities, secure medical supplies and equipment, and safeguard patients.

10. Operational Considerations

a. **Factors That Degrade Security**

- An established routine or pattern of events.
- Inability to restrict access.
- Inability to choose unit location based on security considerations.
- Restrictions on the employment of security forces.
- Required presence of nonunit personnel.
- Inadequate coordination or liaison.

b. **Measures That Enhance Security**

- Continuous reassessment of the mission, policies, threat, and attitude of local inhabitants.
- Using organic and special equipment, such as closed circuit TV, intrusion detection devices, sensors, lighting, barriers, and barricades.
- Assigning physical security responsibilities to trained physical security officers.
- Ensuring that security personnel are aware of guard orders, ROE, local restrictions, and other regulations and policies.
- Maintaining and conducting an aggressive training program, with frequent realistic exercises involving US and HN forces.
- Preparing good defensive positions, barrier plans, and dispersion procedures for vehicles and high-value facilities.
- Maintaining a low off-base personnel profile.
- Restricting access of visitors to the unit location.

SECTION C
OPERATIONS SECURITY

11. Objectives

The OPSEC program is designed to deny access to intelligence and information that the threat can use to learn about plans and operations. The BDOC operations element normally will be the responsible agency for OPSEC, supported by the CI element. OPSEC objectives are to:

a. Avoid stereotyped operations;

b. Understand methods used by the threat to collect intelligence;

c. Deny intelligence and information to the enemy; and

d. Integrate OPSEC into physical and personnel security programs.

12. Measures

Defenders must:

a. Develop essential elements of friendly information on those items and activities of planning and operations that hostile forces can use;

b. Vary locations, routes, and schedules of key activities;

c. Use protective barriers;

d. Check personnel identification at critical entrances;

e. Use additional measures at critical installations, such as communications centers, command posts, and high-density troop areas; and

f. Control schedules of very important persons (VIPs).

13. Intelligence Indicators of Friendly Activity

Activities of base units and personnel may be useful to enemy intelligence agencies.

a. **Operational Indicators**

- Troop restrictions before an operation.
- Increased friendly patrolling and air reconnaissance.
- The complete cessation of friendly patrolling.
- Increased friendly troop movements.
- Special requests for rations, transport, or ammunition.

b. **HUMINT Indicators**

- Media coverage.
- Visits by VIPs.
- Special religious services.
- Bulletins or other notices announcing changes to normal procedures.

c. **Communications Indicators**

- Nonroutine changes to call signs and frequencies.
- Changes in antennas or facilities.
- Increased electronic signature.

14. Reference

Refer to Joint Pub 3-54, "Joint Doctrine for Operational Security," for additional information.

APPENDIX G
TERRORISM

1. General

Terrorism is the unlawful use or threatened use of force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives. Terrorism involves a criminal act that is often symbolic and intended to influence an audience beyond the immediate victims. Terrorist tactics include assassination, arson, bombing, hostage-taking, kidnaping, hijacking and skyjacking, seizure, raids or attacks on facilities, sabotage, hoaxes, potential use of special weapons, and environmental destruction. Combatting terrorism consists of actions, including antiterrorism (defense measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum.

2. Unit Vulnerability

Commanders should evaluate how vulnerable their units are to terrorist attack, including consideration of the HN political environment. Vulnerability changes as units change locations, activities, and quarters, and as reinforcements are available or VIPs conduct visits. Commanders need to update their evaluations continually.

3. Threat Conditions and Responses

Warnings of terrorist activity against US bases normally will come from US intelligence or security authorities or through the security agencies of the HN. Warnings also may come from local police or even from terrorist organizations themselves. In combatting terrorism, bases should use common terrorist threat conditions (THREATCONs), each with its specific security measures and required responses.

a. **Threat Assessment.** Threat assessments will be used to determine threat levels, to implement security decisions, and to establish awareness and resident training requirements. Threat levels are determined by an assessment of the situation using the following six terrorist threat factors.

- **Existence.** A terrorist group is present, assessed to be present, or able to gain access to a given country or locale.
- **Capability.** The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.
- **Intentions.** Recent demonstrated anti-US terrorist activity, or stated or assessed intent to conduct such activity.
- **History.** Demonstrated terrorist activity over time.
- **Targeting.** Current credible information on activity indicative of preparations for specific terrorist operations.
- **Security Environment.** The internal political and security considerations that impact on the capability of terrorist elements to implement their intentions.

b. **Threat Levels.** The severity of the terrorist threat is indicated by the designated threat level, assigned through analysis of the above threat assessment factors. Threat levels and associated factors are listed below.

- **Critical.** Factors of existence, capability, and targeting must be present. History and intentions may or may not be present.

- **High.** Factors of existence, capability, history and intentions must be present.

- **Medium.** Factors of existence, capability, and history must be present. Intentions may or may not be present.

- **Low.** Existence and capability must be present. History may or may not be present.

- **Negligible.** Existence and/or capability may or may not be present.

c. **THREATCON.** The terrorist threat level is one of several factors used in the determination of terrorist THREATCON. Factors that enter into the decision to assign a particular THREATCON and its associated measures include threat, target vulnerability, criticality of assets, security resource availability, impact on operations and morale, damage control, recovery procedures, international regulations, and planned US Government actions that could trigger a terrorist response. The terrorist THREATCON system provides a common framework to facilitate inter-Service coordination, support US military antiterrorist (AT) activities, and enhance overall DOD implementation of US Government AT policy. THREATCONs are described below. Measures and required actions are listed in Joint Pub 3-07.2, "Joint Tactics, Techniques, and Procedures for Antiterrorism."

- **THREATCON NORMAL.** Applies when a general threat of possible terrorist activity exists, but the threat warrants a routine security posture.

- **THREATCON ALPHA.** Applies when there is a general threat of terrorist activity against personnel and installations, the exact nature and extent of which are unpredictable and circumstances do not justify full implementation of THREATCON BRAVO measures. However, base defense forces may have to implement selected measures from higher THREATCONs based on intelligence received. Base defense forces must be able to maintain the measures in this THREATCON indefinitely.

- **THREATCON BRAVO.** Applies when an increased and more predictable threat of terrorist activity exists. Base defense forces must be able to maintain the measures of this THREATCON for weeks without causing undue hardship, without affecting operational capability, and without aggravating relations with local authorities.

- **THREATCON CHARLIE.** Applies when an incident occurs or when intelligence indicates an imminent terrorist action against US bases and personnel. Implementation of measures in the THREATCON for more than a short period probably will create hardship and affect peacetime activities of the unit and its personnel. Sustaining this posture for an extended period probably will require augmentation.

- **THREATCON DELTA.** Applied in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely. Normally, this THREATCON is declared as a localized warning.

4. Base Terrorism Response

The commander of the base is responsible for preventive and protective security measures to protect units and individual Service members and their ability to

accomplish their missions. These measures are described in Appendix F, "Security." Joint Pub 3-07.2, "Joint Tactics, Techniques, and Procedures for Antiterrorism," also describes such measures, as well as techniques for the preparation of a base AT plan.

Intentionally Blank

APPENDIX H
SPECIALIZED EQUIPMENT AND MATERIEL

The following tables listing equipment and materiel specific to joint base defense are not all-inclusive. Base mission, threat, and environment may dictate other requirements. Commanders must ensure that all base defense personnel are properly trained and qualified to use equipment and weapons, as appropriate. SOPs for using equipment and weapons should be developed and implemented.

EQUIPMENT AND MATERIEL FOR GENERAL USE

- Pyrotechnic pistols
- Riot guns
- Tear gas launchers
- Tear gas grenades
- Hand-held flashlights
- Riot helmets
- Shields
- Police batons
- Handcuffs and flexicuffs
- Body armor
- Leg armor
- Vehicle intrusion alarms
- Manuals on local people and customs
- Manuals on threat and person protection
- Trip flares
- Telescopes and tripods
- Infrared devices
- Listening devices
- Protective masks
- Marshalling wands
- Whistles
- Grass-cutting equipment
- Defoliant
- Binoculars
- Firefighting equipment
- Medical equipment and supplies
- Tactical maps—1:50,000 if available out to 35 km
- Ground surveillance equipment
- FLIR on aircraft
- Night vision devices
- Loudspeakers
- Fire extinguishers
- Cameras with flash attachments and tripods
- Telescopic sights
- Photographic filters
- Polaroid cameras
- Hand-held radios
- Tactical deception equipment (camouflage nets, false structures and equipment, false fencing)
- High-pressure hoses and equipment
- Closed circuit television (CCTV) camera
- Low-light-level CCTV camera
- Infrared spotlights and goggles

Figure H-1. Equipment and Materiel for General Use

EQUIPMENT AND MATERIEL FOR ROADBLOCKS AND GATES

Portable lamps, lights	Marker lights	Traffic cones
Traffic signs	Visor sleeves	Tire puncture chains
Lightweight barriers	Mirrors	Portable and stationary metal detectors
Steel cable	Badge system at all entry points	City street maps (1:25000 or 1:15000)
Concertina wire		

Figure H-2. Equipment and Materiel for Roadblocks and Gates

EQUIPMENT AND MATERIEL FOR SEARCHES

Ladders	Safety harnesses	Picks, shovels
Wrecking bars	Flashlights	Magnets
Telescopic mirrors	Hand tools (hammers, pliers, screwdrivers)	Axes
Mine markers	Mine detectors	Helmets
White tape	Saws	Eye shields
Measuring tape	Knives	Chisels
Metal-cutting tools		Mine probes

Figure H-3. Equipment and Materiel for Searches

EQUIPMENT AND MATERIEL FOR SPECIALISTS

- Explosive detectors
- Remote light units
- Remote-controlled EOD devices
- Video periscopes
- Endoscopes
- Concrete mixers
- Portable compressors
- Hydraulic platform
- Engineer tractors
- Engineer heavy equipment
- EOD equipment
- Military working dogs
- NBC detection devices
- Command destruct munitions (thermite grenades)
- Platform hoists

Figure H-4. Equipment and Materiel for Specialists

EQUIPMENT AND MATERIEL FOR STATIC DEFENSE

- Portable sensors
- Portable alarms
- Portable lighting systems
- Barriers (drop arm, swing arm, and counterbalance)
- Roadblock equipment for exit and entry control
- CCTV
- Shot direction indicator
- Wire netting
- Corrugated steel
- Fencing
- Steel girders
- Scaffolding
- Mines (antivehicle, antipersonnel)
- Piping for personnel turnstiles
- Perforated steel planking (PSP) matting
- Duress signal systems at guard stations (doorbell, radio)
- Call to arms system (alarm, loudspeakers)
- Sandbags
- Telephone system and switch backup generators
- Water purification system
- Armor plate glass
- Wire (barbed, concertina)

Figure H-5. Equipment and Materiel for Static Defense

EQUIPMENT AND MATERIEL FOR PORTS

- Minesweeping equipment
- Diving equipment
- Underwater demolition equipment
- Percussion grenades
- Patrol boats
- Underwater salvage equipment
- Minehunting equipment
- Sonar buoys
- Antisubmarine nets
- Antiswimmer nets
- Mines

Figure H-6. Equipment and Materiel for Ports

APPENDIX J
REFERENCES

The development of Joint Pub 3-10.1 is based upon the following primary references.

JOINT PUBLICATIONS

1. Joint Pub 0-2, "Unified Action Armed Forces (UNAAF)."

2. Joint Pub 1-01, "Joint Publication System (Joint Doctrine and JTTP Development Program)."

3. Joint Pub 1-02, "DOD Dictionary of Military and Associated Terms."

4. Joint Pub 2-0, "Joint Doctrine for Intelligence Support to Operations."

5. Joint Pub 3-0, "Doctrine for Joint Operations."

6. Joint Pub 3-01, (In Development) "Joint Doctrine for Countering Air and Missile Threats."

7. Joint Pub 3-01.5, "Doctrine for Joint Theater Missile Defense."

8. Joint Pub 3-07, "Joint Doctrine for Military Operations Other Than War."

9. Joint Pub 3-07.2, "JTTP for Antiterrorism."

10. Joint Pub 3-08, (In Development) "Interagency Coordination During Joint Operations."

11. Joint Pub 3-09, (In Development) "Doctrine for Joint Fire Support."

12. Joint Pub 3-10, "Doctrine for Joint Rear Area Operations."

13. Joint Pub 3-11, "Joint Doctrine for Nuclear, Biological, and Chemical (NBC) Defense."

14. Joint Pub 3-15, "Joint Doctrine for Barriers, Obstacles, and Mine Warfare."

15. Joint Pub 3-52, "Doctrine for Joint Airspace Control in the Combat Zone."

16. Joint Pub 3-53, "Doctrine for Joint Psychological Operations."

17. Joint Pub 3-54, "Joint Doctrine for Operations Security."

18. Joint Pub 3-57, "Doctrine for Joint Civil Affairs."

19. Joint Pub 4-0, "Doctrine for Logistics Support of Joint Operations."

20. Joint Pub 4-01.6, "JTTP for Logistics Over the Shore (JLOTS)."

JOINT WARFIGHTING CENTER PUBLICATION

1. Joint Task Force Commander's Handbook for Peace Operations.

MULTI-SERVICE PUBLICATIONS

1. FM 19-6/AFM 3-3, "Army-Air Force Air Base Ground Defense."

2. FM 90-12/FMFRP 2-73/TACP 50-50/PACAFP 50-50/USAFEP 50-50/AACP 50-50, "Base Defense: Multi-Service Procedures for Defense of a Joint Base."

3. FM 90-23/TACP 50-49/USAFEP 50-49/PACAFP 50-49/AACP 50-49, "Rear Security Operations: Army-Tactical Air Forces Procedures for Rear Security Operations at Echelons Above Corps."

4. FM 100-20/USAF Pamphlet 3-20, "Military Operations in Low Intensity Conflict."

5. DA Pamphlet 525-14/USAF Pamphlet 206-4, "Joint Operational Concept for Air Base Ground Defense."

ARMY PUBLICATIONS

1. AR 381-10, "US Army Intelligence Activities."

2. AR 381-12, "Subversion and Espionage Directed Against the US Army (SAEDA)."

3. AR 381-19, "Intelligence Dissemination and Production Support."

4. AR 381-20, "US Army Counterintelligence Activities."

5. AR 525-13, "The Army Combating Terrorism Program."

6. AR 530-1, "Operations Security."

7. FM 1-103, "Airspace Management and Army Air Traffic Control in a Combat Zone."

8. FM 3-4, "NBC Protection."

9. FM 3-5, "NBC Decontamination."

10. FM 3-100, "NBC Defense, Chemical Weapons, Smoke and Flame Operations."

11. FM 5-34, "Engineer Field Data."

12. FM 5-116, "Engineer Operations: Echelons Above Corps."

13. FM 6-20, "Fire Support in the AirLand Battle."

14. FM 6-20-30, “Fire Support for Corps and Division Operations.”

15. FM 6-30, “Tactics, Techniques and Procedures for Observed Fire.”

16. FM 7-8, “The Infantry Platoon and Squad (Infantry, Airborne, Air Assault, Ranger).”

17. FM 7-10, “The Infantry Rifle Company (Infantry, Airborne, Air Assault, Ranger).”

18. FM 7-20, “The Infantry Battalion (Infantry, Airborne and Air Assault).”

19. FM 7-30, “Infantry, Airborne, and Air Assault Brigade Operations.”

20. FM 11-23, “Theater Communications Command.”

21. FM 19-1, “Military Police Support for the AirLand Battle.”

22. FM 22-6, “Guard Duty.”

23. FM 31-20-3, “Foreign Internal Defense, Tactics, Techniques, and Procedures for Special Forces.”

24. FM 33-1, “Psychological Operations.”

25. FM 34-1, “Intelligence and Electronic Warfare Operations.”

26. FM 34-2, “Collection Management.”

27. FM 34-3, “Intelligence Analysis.”

28. FM 34-37, “Echelons Above Corps (EAC) Intelligence and Electronic Warfare Operations.”

29. FM 34-52, “Intelligence Interrogation.”

30. FM 34-60, “Counterintelligence.”

31. FM 34-130, “Intelligence Preparation of the Battlespace.”

32. FM 41-10, “Civil Affairs Operations.”

33. FM 44-18, “Air Defense Artillery Employment, Stinger.”

34. FM 44-31, “Tactics, Techniques, and Procedures for Avenger Squad Operations.”

35. FM 44-63, “FAAD/SHORAD Battalion Operations, Heavy Divisions.”

36. FM 44-85, “Patriot Battalion and Battery Operations.”

37. FM 44-100, "US Army Air Defense Operations."

38. FM 54-40, "Area Support Group."

39. FM 63-4, "Combat Service Support Operations: Theater Army Area Command."

40. FM 71-100, "Division Operations."

41. FM 90-14, "Rear Battle."

42. FM 100-5, "Operations."

43. FM 100-15, "Corps Operations."

44. FM 100-16, "Support Operations: Echelons Above Corps."

45. FM 101-5, "Staff Organization and Operations."

AIR FORCE PUBLICATIONS

1. Air Force Manual 2-11, "Air Force Foreign Internal Defense Operations."

2. Air Force Pamphlet 31-302, "Air Base Ground Defense and Contingency Operations."

3. Air Force Pamphlet 360-2, "Wing Commander's Air Base Operability (ABO) Planning Considerations Guide."

4. Air Force Instruction 31-301, "Air Base Ground Defense Tactical Doctrine."

5. Air Force Regulation 355-1, "Disaster Preparedness Planning and Operations."

6. Air Force Regulation 355-3, "Air Force Personnel Shelter Program."

7. Air Force Regulation 355-8, "Mission Oriented Protective Postures."

8. Air Force Regulation 360-1, "Air Base Operability — Planning and Operations."

NAVY PUBLICATIONS

1. NWP 8, "Command and Control."

2. NWP 15-2, "Special Boat Squadrons in Naval Special Warfare."

3. NWP 39, "Naval Coastal Warfare Doctrine."

4. NWP 40, "Inshore Undersea Warfare."

MARINE CORPS PUBLICATIONS

1. FMFM 8-3, “Advanced Naval Base Defense.”

2. OH 2-6, “MAGTF Rear Area Security.”

Intentionally Blank

APPENDIX K
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to the Joint Warfighting Center, Attn: Doctrine Division, Fenwick Road, Bldg 96, Fort Monroe, VA 23651-5000. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent for this publication is the US Army. The Joint Staff doctrine sponsor for this publication is the Director for Operational Plans and Interoperability (J-7).

3. Supersession

This publication supersedes Joint Pub 3-10.1, 15 March 1993, "Joint Tactics, Techniques, and Procedures for Base Defense."

4. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: CSA WASHINGTON DC//DAMO-FDQ//
INFO: JOINT STAFF WASHINGTON DC//J7-JDD//

Routine changes should be submitted to the Director for Operational Plans and Interoperability (J-7), JDD, 7000 Joint Staff Pentagon, Washington, D.C. 20318-7000.

b. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Military Services and other organizations are requested to notify the Director, J-7, Joint Staff, when changes to source documents reflected in this publication are initiated.

c. Record of Changes:

CHANGE NUMBER	COPY NUMBER	DATE OF CHANGE	DATE ENTERED	POSTED BY	REMARKS

5. Distribution

a. Additional copies of this publication can be obtained through Service publication centers.

b. Only approved pubs and test pubs are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attache Office) to DIA Foreign Liaison Office, PSS, Room 1A674, Pentagon, Washington D.C. 20301-7400.

c. Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 1 November 1988, "Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands."

By Military Services:

Army:	US Army AG Publication Center 2800 Eastern Boulevard Baltimore, MD 21220-2898
Air Force:	Air Force Publications Distribution Center 2800 Eastern Boulevard Baltimore, MD 21220-2896
Navy:	CO, Naval Inventory Control Point 700 Robbins Avenue Bldg 1, Customer Service Philadelphia, PA 19111-5099
Marine Corps:	Marine Corps Logistics Base Albany, GA 31704-5000
Coast Guard:	Coast Guard Headquarters, COMDT (G-OPD) 2100 2nd Street, SW Washington, D.C. 20593-0001

d. Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified joint publications must be in accordance with DOD Regulation 5200.1-R.

GLOSSARY
PART I—ABBREVIATIONS AND ACRONYMS

AADC	area air defense commander
ACA	airspace control authority
ADC	area damage control
AFOSI	Air Force Office of Special Investigations
ALSS	naval advanced logistic support site
AO	area of operations
ASG	area support group
AT	antiterrorism
BCOC	base cluster operations center
BDOC	base defense operations center
BDZ	base defense zone
C2	command and control
C4	command, control, communications, and computers
CA	civil affairs
CI	counterintelligence
CINC	commander of a combatant command; commander in chief
COMMARFOR	Commander, Marine Forces
DOD	Department of Defense
DZ	drop zone
EOD	explosive ordnance disposal
EPW	enemy prisoner of war
EW	electronic warfare
FLS	naval forward logistic site
FSCC	Fire Support Coordination Center
FSE	fire support element
HDC	harbor defense commander
HN	host nation
HNS	host-nation support
HUMINT	human intelligence
IFF	identification, friend or foe
JFC	joint force commander
JRA	joint rear area
JRAC	joint rear area coordinator
JRTOC	Joint Rear Tactical Operations Center
LNO	liaison officer

LP	listening post
LZ	landing zone
MAGTF	Marine air-ground task force
MCM	mine countermeasures
MDSU	mobile diving and salvage unit
MP	military police
NBC	nuclear, biological, and chemical
NCWC	naval coastal warfare commander
OP	observation post
OPCON	operational control
OPSEC	operations security
PA	public affairs
PIR	priority intelligence requirements
PSHDGRU	port security and harbor defense group
PSU	port security unit
PSYOP	psychological operations
RAOC	rear area operations center
ROE	rules of engagement
RTOC	Rear Tactical Operations Center
SBU	special boat unit
SOFA	status-of-forces agreement
SOP	standing operating procedure
TAACOM	theater army area command
TACON	tactical control
TCF	tactical combat force
THREATCON	threat condition
UN	United Nations
VIP	very important person

airspace control authority. The commander designated to assume overall responsibility for the operation of the airspace control system in the airspace control area. (Joint Pub 1-02)

area air defense commander. Within a unified command, subordinate unified command, or joint task force, the commander will assign overall responsibility for air defense to a single commander. Normally, this will be the component commander with the preponderance of air defense capability and the command, control, and communications capability to plan and execute integrated air defense operations. Representation from the other components involved will be provided, as appropriate, to the area air defense commander's headquarters. Also called AADC. (Joint Pub 1-02)

area damage control. Measures taken before, during, or after hostile action or natural or man-made disasters, to reduce the probability of damage and minimize its effects. (Joint Pub 1-02)

area of operations. An operational area defined by the joint force commander for land and naval forces. Areas of operation do not typically encompass the entire operational area of the joint force commander, but should be large enough for component commanders to accomplish their missions and protect their forces. (Joint Pub 1-02)

area of responsibility. 1. The geographical area associated with a combatant command within which a combatant commander has authority to plan and conduct operations. 2. In naval usage, a predefined area of enemy terrain for which supporting ships are responsible for covering by fire on known targets or targets of opportunity and by observation. Also called AOR. (Joint Pub 1-02)

base. 1. A locality from which operations are projected or supported. 2. An area or locality containing installations which provide logistic or other support. 3. Home airfield or home carrier. (Joint Pub 1-02)

base cluster. In base defense operations, a collection of bases, geographically grouped for mutual protection and ease of command and control. (Joint Pub 1-02)

base cluster commander. In base defense operations, the senior officer in the base cluster (excluding medical officers, chaplains, and commanders of transient units), with responsibility for coordinating the defense of bases within the base cluster, and for integrating base defense plans of bases into a base cluster defense plan. (Joint Pub 1-02)

base cluster operations center. A command and control facility that serves as the base cluster commander's focal point for defense and security of the base cluster. (Joint Pub 1-02)

base commander. In base defense operations, the officer assigned to command a base. (Joint Pub 1-02)

base defense. The local military measures, both normal and emergency, required to nullify or reduce the effectiveness of enemy attacks on, or sabotage of, a base, to ensure that the maximum capacity of its facilities is available to US forces. (Joint Pub 1-02)

base defense forces. Troops assigned or attached to a base for the primary purpose of base defense and security, and augmentees and selectively armed personnel available to the base commander

for base defense from units performing primary missions other than base defense. (Joint Pub 1-02)

base defense operations center. A command and control facility established by the base commander to serve as the focal point for base security and defense. It plans, directs, integrates, coordinates, and controls all base defense efforts, and coordinates and integrates into area security operations with the rear area operations center/rear tactical operations center. (Joint Pub 1-02)

base defense zone. An air defense zone established around an air base and limited to the engagement envelope of short-range air defense weapons systems defending that base. Base defense zones have specific entry, exit, and identification, friend or foe procedures established. Also called BDZ. (Joint Pub 1-02)

civil affairs. The activities of a commander that establish, maintain, influence, or exploit relations between military forces and civil authorities, both governmental and nongovernmental, and the civilian populace in a friendly, neutral, or hostile area of operations in order to facilitate military operations and consolidate operational objectives. Civil affairs may include performance by military forces of activities and functions normally the responsibility of local government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. (Joint Pub 1-02)

coastal sea control. The employment of forces to ensure the unimpeded use of an offshore coastal area by friendly forces and, as appropriate, to deny the use of the area to enemy forces. (Joint Pub 1-02)

host-nation support. Civil and/or military assistance rendered by a nation to foreign forces within its territory during peacetime, crises or emergencies, or war based on agreements mutually concluded between nations. (Joint Pub 1-02)

joint base. For purposes of base defense operations, a joint base is a locality from which operations of two or more of the Military Departments are projected or supported and which is manned by significant elements of two or more Military Departments or in which significant elements of two or more Military Departments are located. (Joint Pub 1-02)

joint rear area. A specific land area within a joint force commander's operational area designated to facilitate protection and operation of installations and forces supporting the joint force. (Joint Pub 1-02)

joint rear area coordinator. The officer with responsibility for coordinating the overall security of the joint rear area in accordance with joint force commander directives and priorities in order to assist in providing a secure environment to facilitate sustainment, host nation support, infrastructure development, and movements of the joint force. The joint rear area coordinator also coordinates intelligence support and ensures that area management is practiced with due consideration for security requirements. Also called JRAC. (Joint Pub 1-02)

joint rear area operations. Those operations in the joint rear area that facilitate protection or support of the joint force. (Approved for inclusion in the next edition of Joint Pub 1-02.)

joint rear tactical operations center. A joint operations cell tailored to assist the joint rear area coordinator in meeting mission responsibilities. Also called JRTOC. (Joint Pub 1-02)

naval coastal warfare area. An assigned geographic area of operations which includes offshore waters, harbor approaches, harbors, ports, waterfront facilities, and those internal waters and rivers which provide access to port facilities. (Approved for inclusion in the next edition of Joint Pub 1-02.)

naval coastal warfare commander. An officer designated to conduct naval coastal warfare missions within a designated naval coastal geographic area. Also called NCWC. (Joint Pub 1-02)

nongovernmental organizations. Transnational organizations of private citizens that maintain a consultative status with the Economic and Social Council of the United Nations. Nongovernmental organizations may be professional associations, foundations, multinational businesses, or simply groups with a common interest in humanitarian assistance activities (development and relief). "Nongovernmental organizations" is a term normally used by non-United States organizations. Also called NGO. (Joint Pub 1-02)

operational control. Transferable command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority). Operational control may be delegated and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions. Operational control does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called OPCON. (Joint Pub 1-02)

operational environment. A composite of the conditions, circumstances, and influences which affect the employment of military forces and bear on the decisions of the unit commander. Some examples are: a. permissive environment--operational environment in which host country military and law enforcement agencies have control and the intent and capability to assist operations that a unit intends to conduct. b. uncertain environment--operational environment in which host government forces, whether opposed to or receptive to operations that a unit intends to conduct, do not have totally effective control of the territory and population in the intended area of operations. c. hostile environment--operational environment in which hostile forces have control and the intent and capability to effectively oppose or react to the operations a unit intends to conduct. (Joint Pub 1-02)

private voluntary organizations. Private, nonprofit humanitarian assistance organizations involved in development and relief activities. Private voluntary organizations are normally United States-based. "Private voluntary organization" is often used synonymously with the term "nongovernmental organizations." Also called PVO. (Joint Pub 1-02)

psychological operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. (Joint Pub 1-02)

rear area. For any particular command, the area extending forward from its rear boundary to the rear of the area assigned to the next lower level of command. This area is provided primarily for the performance of support functions. (Joint Pub 1-02)

rear area operations center/rear tactical operations center. A command and control facility that serves as an area/subarea commander's planning, coordinating, monitoring, advising, and directing agency for area security operations. (Joint Pub 1-02)

response force. A mobile force with appropriate fire support designated, usually by the area commander, to deal with Level II threats in the rear area. (Joint Pub 1-02)

short-range air defense engagement zone. See weapon engagement zone. (Joint Pub 1-02)

status-of-forces agreement. An agreement which defines the legal position of a visiting military force deployed in the territory of a friendly state. Agreements delineating the status of visiting military forces may be bilateral or multilateral. Provisions pertaining to the status of visiting forces may be set forth in a separate agreement, or they may form a part of a more comprehensive agreement. These provisions describe how the authorities of a visiting force may control members of that force and the amenability of the force or its members to the local law or to the authority of local officials. To the extent that agreements delineate matters affecting the relations between a military force and civilian authorities and population, they may be considered as civil affairs agreements. Also called SOFA. (Joint Pub 1-02)

tactical area of responsibility. None. (Upon approval of this revision, this term and its definition will be deleted from Joint Pub 1-02)

tactical combat force. A combat unit, with appropriate combat support and combat service support assets, that is assigned the mission of defeating Level III threats. (Joint Pub 1-02)

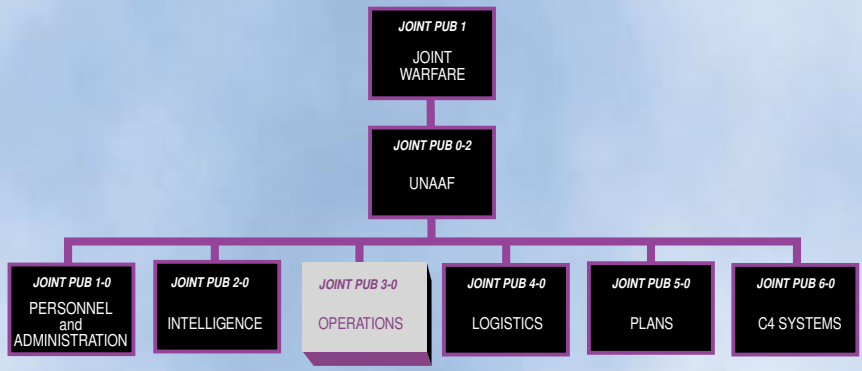
tactical control. Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed and, usually, local direction and control of movements or maneuvers necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of combatant command. Also called TACON. (Joint Pub 1-02)

weapon engagement zone. In air defense, airspace of defined dimensions within which the responsibility for engagement of air threats normally rests with a particular weapon system. Also called WEZ. a. fighter engagement zone. In air defense, that airspace of defined dimensions within which the responsibility for engagement of air threats normally rests with fighter aircraft. Also called FEZ. b. high-altitude missile engagement zone. In air defense, that airspace of defined dimensions within which the responsibility for engagement

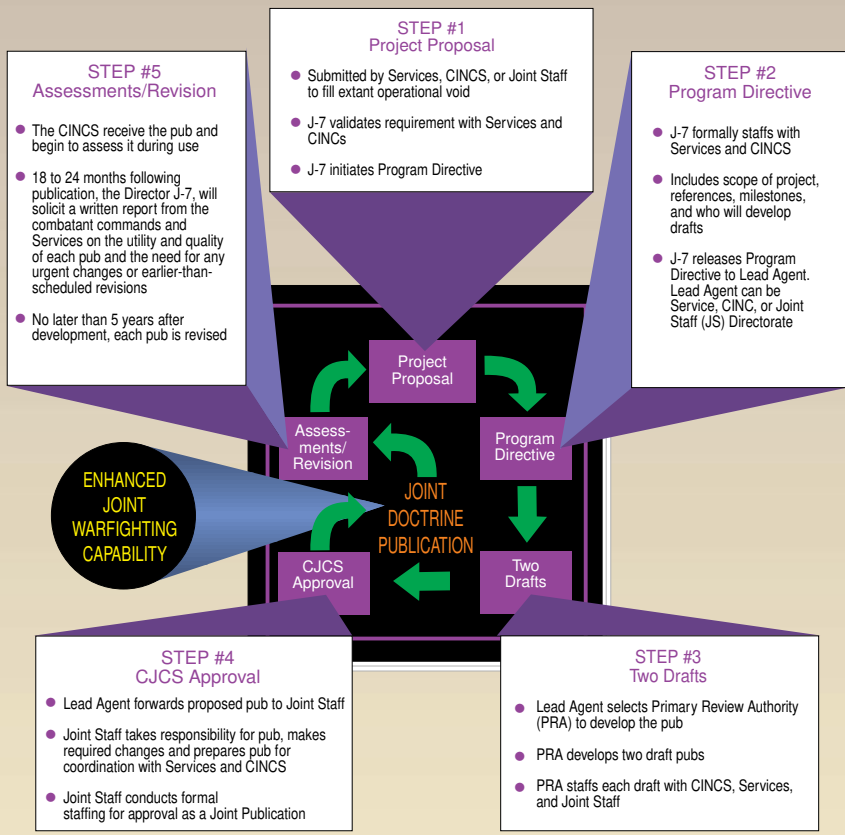
of air threats normally rests with high-altitude surface-to-air missiles. Also called HIMEZ. c. low-altitude missile engagement zone. In air defense, that airspace of defined dimensions within which the responsibility for engagement of air threats normally rests with low- to medium-altitude surface-to-air missiles. Also called LOMEZ. d. short-range air defense engagement zone. In air defense, that airspace of defined dimensions within which the responsibility for engagement of air threats normally rests with short-range air defense weapons. It may be established within a low- or high-altitude missile engagement zone. Also called SHORADEZ. e. joint engagement zone. In air defense, that airspace of defined dimensions within which multiple air defense systems (surface-to-air missiles and aircraft) are simultaneously employed to engage air threats. Also called JEZ. (Joint Pub 1-02)

Intentionally Blank

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint doctrine and tactics, techniques, and procedures are organized into a comprehensive hierarchy as shown in the chart above. **Joint Pub 3-10.1** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:


STEP #1
Project Proposal
Submitted by Services, CINCS, or Joint Staff to fill extant operational void
J-7 validates requirement with Services and CINCs
J-7 initiates Program Directive
STEP #2
Program Directive
J-7 formally staffs with Services and CINCS
Includes scope of project, references, milestones, and who will develop drafts
J-7 releases Program Directive to Lead Agent. Lead Agent can be Service, CINC, or Joint Staff (JS) Directorate
STEP #5
Assessments/Revision
The CINCS receive the pub and begin to assess it during use
18 to 24 months following publication, the Director J-7, will solicit a written report from the combatant commands and Services on the utility and quality of each pub and the need for any urgent changes or earlier-than-scheduled revisions
No later than 5 years after development, each pub is revised
Project Proposal
Program Directive
Two Drafts
CJCS Approval
Assess-ments/ Revision
JOINT DOCTRINE PUBLICATION
ENHANCED JOINT WARFIGHTING CAPABILITY
STEP #3
Two Drafts
Lead Agent selects Primary Review Authority (PRA) to develop the pub
PRA develops two draft pubs
PRA staffs each draft with CINCS, Services, and Joint Staff
STEP #4
CJCS Approval
Lead Agent forwards proposed pub to Joint Staff
Joint Staff takes responsibility for pub, makes required changes and prepares pub for coordination with Services and CINCS
Joint Staff conducts formal staffing for approval as a Joint Publication

JOINT
CHIEFS OF STAFF